VAL 15-000-3740

UNITED STATES ENVIRONMENTAL PROTECTION AGENCY
WASHINGTON, D.C. 20460

DEC 2 3 2014

OFFICE OF THE
CHIEF FINANCIAL OFFICER

The Honorable Harold Rogers
Chairman
Committee on Appropriations
U.S. House of Representatives
Washington, D.C. 20515

Dear Mr. Chairman:

I am transmitting the U.S. Environmental Protection Agency's response to the September 2014 Government Accountability Office report entitled, *Data Center Consolidation Reporting Can Be Improved to Reflect Substantial Planned Savings* (GAO-14-713). The EPA prepared this response pursuant to 31 U.S.C. 720.

The EPA generally agrees with the findings, conclusions, and recommendations in the GAO report. The report contains four recommendations overall, with one of the recommendations directed to the EPA (and several other federal agencies). The EPA provides its response to that recommendation below.

Recommendation:

The Secretaries of Agriculture, Commerce, Defense, Energy, the Interior, Transportation, the Treasury, and Department of Veterans Affairs; the Administrators of the Environmental Protection Agency and NASA; and the Director of the Office of Personnel Management should direct responsible officials to report all data center consolidation cost savings and avoidances to [the Office of Management and Budget] OMB in accordance with established guidance.

EPA Response:

The EPA's National Computing Center, responsible for leading the agency's data center consolidation efforts, pulls together consolidation cost savings information that is sent quarterly to the OMB as a part of the OMB's PortfolioStat Integrated Data Call submission. The EPA will continue this process for future iterations of the OMB's data calls.

Thank you for the opportunity to review and comment on the GAO's final report. If you have any further questions, please contact me or your staff may contact James Blizzard in the EPA's Office of Congressional and Intergovernmental Relations, by phone at (202) 564-1695, or by email at blizzard.james@epa.gov.

Sincerely,

David A. Bloom
Acting Chief Financial Officer

AL 12-000-5979

UNITED STATES ENVIRONMENTAL PROTECTION AGENCY
WASHINGTON, D.C. 20460

MAR 3 0 2012

THE ADMINISTRATOR

The Honorable Harold Rogers
Chairman
Committee on Appropriations
U.S. House of Representatives
Washington, DC 20515

Dear Mr. Chairman:

I am pleased to renew the charter of the Human Studies Review Board in accordance with the provisions of the Federal Advisory Committee Act, 5 U.S.C. App. 2. The Human Studies Review Board is in the public interest and supports the U.S. Environmental Protection Agency in performing its duties and responsibilities.

I am filing the enclosed charter with the Library of Congress. The board will be in effect for two years from the date the charter is filed with Congress. After two years, the charter may be renewed as authorized in accordance with Section 14 of FACA (5 U.S.C. App. 2 § 14).

If you have any questions or require additional information, please contact me or your staff may contact Clara Jones in the EPA's Office of Congressional and Intergovernmental Relations at (202) 564-3701.

Sincerely,

Lisa P. Jackson

Enclosure

12-000-5979

UNITED STATES ENVIRONMENTAL PROTECTION AGENCY CHARTER

HUMAN STUDIES REVIEW BOARD

1. Committee's Official Designation (Title):

Human Studies Review Board

2. Authority:

This charter renews the Human Studies Review Board (HSRB) in accordance with the provisions of the Federal Advisory Committee Act (FACA), 5 U.S.C. App. 2. HSRB is in the public interest and supports EPA in performing its duties and responsibilities.

3. Objectives and Scope of Activities:

The HSRB will provide advice, information, and recommendations on issues related to scientific and ethical aspects of human subjects research.

The major objectives are to provide advice and recommendations on:

a. Research Proposals and Protocols;

b. Reports of completed research with human subjects; and

c. How to strengthen EPA's programs for protection of human subjects of research.

4. Description of Committees Duties:

The duties of the HSRB are solely to provide scientific or policy advice to EPA.

5. Official(s) to Whom the Committee Reports:

HSRB will report to the EPA Administrator through EPA's Science Advisor.

6. Agency Responsible for Providing the Necessary Support:

EPA will be responsible for financial and administrative support. Within EPA, this support will be provided by the Office of the Science Advisor (OSA).

7. Estimated Annual Operating Costs and Person Years:

The estimated annual operating cost of HSRB is $850,000 which includes 3.0 person-years of support.

8. Designated Federal Officer:

A full-time or permanent part-time employee of EPA will be appointed as the DFO. The DFO or a designee will be present at all of the advisory committee's and subcommittee meetings. Each meeting will be conducted in accordance with an agenda approved in advance by the DFO. The DFO is authorized to adjourn any meeting when he or she determines it is in the public interest to do so, and will chair meetings when directed to do so by the official to whom the committee reports.

9. Estimated Number and Frequency of Meetings:

The Committee expects to meet approximately four (4) times a year. Meetings may occur approximately once every three (3) months or as needed and approved by the Designated Federal Officer (DFO). EPA may pay travel and per diem expenses when determined necessary and appropriate.

As required by FACA, HSRB will hold open meetings unless the EPA Administrator determines that a meeting or a portion of a meeting may be closed to the public in accordance with subsection c of section 552b of title 5, United States Code. Interested persons may attend meetings, appear before the Board as time permits, and file comments with the HSRB.

10. Duration and Termination:

This charter will be in effect for two years from the date it is filed with Congress. After this two-year period, the charter may be renewed as authorized in accordance with Section 14 of FACA.

11. Member Composition:

The HSRB will be composed of approximately thirteen (13) members who will serve as Special Government Employees (SGEs) or Regular Government Employees (RGEs). In selecting members, the EPA will consider candidates from the environmental scientific/technical fields, human health care professionals, academia, industry, public and private research institutes or organizations, other governmental agencies, and other relevant interest areas. The HSRB membership will include experts in relevant scientific or technical disciplines such as bioethics, biostatistics, human health risk assessment and human toxicology.

12-000-5979

12. **Subgroups:**

EPA, or the HSRB with EPA's approval, may form HSRB subcommittees or workgroups for any purpose consistent with this charter. Such subcommittees or workgroups may not work independently of the chartered committee and must report their recommendations and advice to the HSRB for full deliberation and discussion. Subcommittees or workgroups have no authority to make decisions on behalf of the chartered committee nor can they report directly to the Agency.

13. **Recordkeeping:**

The records of the Committee, formally and informally established subcommittees, or other subgroups of the Committee, shall be handled in accordance with NARA General Records Schedule 26, Section 2 and EPA Records Schedule 181 or other approved agency records disposition schedule. Subject to the Freedom of Information Act, 5 U.S.C. 552, these records shall be available for public inspection and copying, in accordance with the Federal Advisory Committee Act.

March 28, 2012
Agency Approval Date

_____
Date Filed with Congress

AL 13-000-3367

UNITED STATES ENVIRONMENTAL PROTECTION AGENCY
WASHINGTON, D.C. 20460

MAR 28 2013

OFFICE OF THE
CHIEF FINANCIAL OFFICER

The Honorable Harold Rogers
Chairman
Committee on Appropriations
U.S. House of Representatives
Washington, D.C. 20515

Dear Mr. Chairman:

I am transmitting the U.S. Environmental Protection Agency's response to the July 2012 Governmental Accountability Office report entitled, *Information Security: Environmental Protection Agency Needs to Resolve Weaknesses,* GAO-12-530SU. The EPA prepared this response pursuant to 31 U.S.C. 720.

The GAO was asked to determine whether the agency has effectively implemented appropriate information security controls to protect the confidentiality, integrity, and availability of the information and systems that support its mission. Specifically, the GAO provided the EPA with 94 recommendations designed to enhance access and other information security controls over the EPA's information systems. The EPA is in agreement with the spirit of these findings and recommendations and is currently taking action to implement the recommendations.

Enclosed is the EPA's response to each recommendation. The responses reflect the EPA's continuing efforts to ensure that all information assets are protected at a level that is commensurate with the sensitivity level of the data. The EPA appreciates the GAO's review of its Information Security Program and the opportunity to respond to the final report.

If you have any questions, please contact me or your staff may call Christina Moody, in the EPA's Office of Congressional and Intergovernmental Relations at (202) 564-0260.

Sincerely,

Barbara J. Bennett
Chief Financial Officer

Enclosure

13-000-3367

Enclosure - GAO Information Security Engagement (GAO-12-530SU)

BOUNDARY PROTECTION

Public Access Networks - EPA did not adequately segregate its internal networks from public access. NIST guidance states that organizations should provide adequate protection for their networks and employ information control policies and enforcement mechanisms to control the flow of information between designated sources and destinations within an information system. However, we were able to reach critical internal network and system management assets from an EPA public library at the Research Triangle Park location. Access obtained included a TACACS+[1] console for managing EPA network devices, a network management server, and a network logging server. Although EPA had employed physical access controls to library facilities, the risk remains that the public could gain access to internal systems through library computer systems.

GAO Recommendation:

1. Restrict library networks from being used to gain unauthorized access into internal EPA networks.

EPA Response:

The EPA concurs with the recommendation. The procedures for accessing EPA-RTP library patron computers have been modified as follows:

1. Only EPA staff and contractors with EPA LAN userids and passwords can access the patron computers.
2. Members of the public wishing to visit the library must follow the steps below:
   - The visitor must first go through building security before being escorted into the library.
   - Once in the library, the patron must sign in as a library visitor.
   - The visitor will then consult with a library staff person who assesses their need. If it is determined that a member of the public requires information from an online resource that is available through a publicly available or other authorized website, a library staff person logs onto a patron computer using a station-restricted EPA userid and password. The library staff person then performs any necessary information searches for the patron. At no time is the visitor allowed to operate the EPA computer or gain access to the EPA network.

It is estimated that on an annual basis fewer than five members of the public visit the library for the purpose of obtaining online resource materials. For EPA procedures that govern public access to library materials please see EPA Classification No.: CIO 2170.2-P-12.0 for the document titled EPA Library Public Access Procedures, http://www.epa.gov/irmpoli8/policies/public_access_procedures.pdf.

3. EPA is taking action to separate the headquarters library network from the headquarters' network.

[1] TACACS+ is a Cisco proprietary protocol that provides access control for routers, network access servers, and other network computing devices via one or more centralized servers. TACACS+ also provides separate authentication, authorization, and accounting services.

SSH Inbound Connections - EPA allowed inbound use of the encrypted protocol, Secure Shell (SSH), for the e-Rulemaking initiative's[2] Federal Docket Management System without adequate authorization.[3] NIST guidance states that system-specific controls are the primary responsibility of information system owners and their respective authorizing officials, and should be configured to the most restrictive mode consistent with operational requirements. However, EPA allowed unrestricted inbound SSH connections that were not approved by the system owner's authorizing official. The stated purpose for the firewall rule established for the connection is for agencies to be able to transfer batches of scanned documents over a secure connection. As a result, any port or protocol could be forwarded from the internal network through the encrypted tunnel where an inbound connection could be used to remotely control and provide access to the internal network from any Internet location.

GAO Recommendations:
2. Restrict the use of SSH inbound connections for the e-Rulemaking initiative's Federal Docket Management System to that consistent with operational requirements.
3. Provide appropriate authorization(s) for inbound use of SSH for the e-Rulemaking initiative's Federal Docket Management System.

EPA Response:
The EPA will update the SDWIS security plan to reflect current policies and procedures per Agency standards and NIST 800-18 guidance.

IDENTIFICATION AND AUTHENTICATION

Cisco Wireless Access Control Server Password Policy - EPA did not implement sufficient password policy controls on its Cisco wireless access control server at EPA headquarters. NIST guidance on password management states that agencies are to establish password complexity and lifetime restrictions for passwords on information systems. Additionally, agency policy states that passwords should be changed at least every 90 days. However, EPA did not provide sufficient password policy controls to manage access to its Cisco wireless access control server at EPA headquarters. This server is used to establish wireless network encrypted sessions that also provide access into EPA's production network[4] and enable wireless users' authentication to EPA's Active Directory. For example, we found the following policy violations:

- Password setting allowed for use of username and a default password.
- Password length was set to a minimum length of 4 characters.
- Password complexity settings were not enabled.
- Passwords had no maximum lifetime requirements set.

---

[2] The eRulemaking Initiative's Federal Docket Management System is an online public docket and comment system being implemented to expand public access to and the ability to comment on federal agencies' rulemaking activities. It facilitates the submission of public comments to federal agencies' rulemaking dockets by allowing the public to comment online. While the Federal Docket Management System is a centralized system, each federal agency is the sole owner of its data and each agency manages its internal users' access and roles within the system as well as the posting of data on the system as part of its rulemaking procedures.

[3] This protocol is used for remote access and communicating over the Internet and allows users to bypass firewall and network-based monitoring controls.

[4] Per EPA's wireless standard configuration document, wireless networks, because of the economies of scale in implementation, are used to extend employees' reach into the agency's production network.

13-000-3367

As a result, the EPA wireless access control server is vulnerable to compromise, which could enable an attacker to create a new user account profile that could bypass EPA's centralized Active Directory authentication and encryption and be used to initiate unauthorized sessions into EPA wireless networks.

GAO Recommendation:
4. Establish password controls for password length, complexity, and lifetime requirements in accordance with EPA policy.

EPA Response:
The EPA concurs with the recommendation and has corrected the weakness. All security concerns regarding Wireless Access Control Server Password policy have been addressed. All Policies are created off of NIST standards and DoD STIG guidelines and recommendations, as well as industry standards.

TACACS+ Password Policy – EPA did not effectively manage password policy on its TACACS+ server. NIST guidance on procedures to implement identification and authentication policy states that agencies should establish minimum password complexity requirements, such as number of characters and ix of upper case letters, lower case letters, numbers, and special characters, including minimum requirements for each type, and should define and enforce password minimum and maximum lifetime restrictions and prohibitions on password reuse. Additionally, agency policy states that passwords should be changed at least every 90 days. However, account policies were not effectively implemented in accordance with policy, as the following examples illustrate:

- The default for password length was set to a minimum of 4 characters.
- Passwords were not required to have any complexity.
- Password expiration was not applied to a cisco access control server account and a local operating system administrative account.

Without strong password policies, EPA's TACACS+ system and network resources are at increased risk of compromise.

GAO Recommendation:
5. Establish controls for password length, complexity, and expiration for the TACACS+ server.

EPA Response:
The EPA concurs with the recommendation and has corrected the weakness. The EPA conducted a thorough review of settings and made corrections to the TACACS settings to reflect:

- Administrator Password has been set to a minimum of 8 characters;
- The password complexity has been set to – Passwords must contain upper, lower, non-alphabetic and numeric characters; and
- All accounts have been verified to have password expiration in place. NSOC developed a TACACS SOP [NSO-SOP-006 TACACS Administration] which specifies "The password policy for TACACS administrators requires a minimum of 8 characters, and must contain a lowercase alphabetic character, an upper case character, and one numeric character. Users' passwords expire every 90 days with a 5 day warning that the password will expire and a 5 day grace period that the password can still be changed."

Shared Account - A privileged local operating system account on the TACACS+ server had shared administrative privileges. NIST provides guidance on procedures to facilitate the implementation of the identification and authentication policy, which includes assigning unique identifiers to users.

Additionally, agency policy states that information managers should create unique system accounts for each authorized user. However, a local operating system administrative account on the TACACS+ server was shared, and the password had not been changed in more than 2 years. As a result, individual accountability could be lost in monitoring for authorized as well as unauthorized system activity.

GAO Recommendation:
6. Remove the shared account if there is not a valid business need to share the account; if the account remains, change the password on a regular basis.

EPA Response:
The EPA concurs with the recommendation and has corrected the weakness. The EPA reviewed all shared accounts and removed all shared accounts that were not required for daily operations. There are no local accounts in the local administrator's group. Only individual and service domain accounts have local administer privileges. The EPA also developed a SOP to address shared accounts: " Shared, group, or custodial UserIDs are not allowed."

Oracle Database Passwords - EPA had not implemented sufficient password controls for many of its Oracle production database systems. NIST guidance states that complex passwords should be established in systems to reduce the likelihood of a successful attack. However, EPA did not require or enforce complex passwords for its databases that support EPA applications, as illustrated in these examples:

- Active user accounts on the databases supporting CBITS, the Central Data Exchange (CDX), and Oracle's Collaboration Suite (OCS)[5]had default or weak passwords. This included those for database administrator roles supporting these applications, one user account with a default password, and two user accounts with weak passwords.
- Failed login attempts were not limited on the CBITS systems in the Oracle monitoring profile that includes sensitive privileged accounts.
- Password life and password verify functions had not been enabled in default and system profiles that included privileged accounts for 13 database systems in support of CBITS, CDX, and Electronic Greenhouse Gas Reporting Tool (e-GGRT),[6] CERCLIS, [7] Superfund Enterprise Management System (SEMS)[8], and Oracle's Application Server[9]Infrastructure and Collaboration Suite (OAS/OCS) applications.

As a result, heightened risk exists that unauthorized individuals could exploit these vulnerabilities to guess passwords and use them to obtain unauthorized access to EPA databases.

[5] SOCS is a suite of communication and collaboration applications that allows internal group sharing of information through, for example, establishing team workspaces for content services,
[6] The e-GGRT is a web-based system EPA developed to support reporting under the Greenhouse Gas Reporting Program.
[7] CERCLIS is the official repository for site- and non-site-specific Superfund data in support of the Comprehensive Environmental Response, Compensation, and Liability Act of 1980. It contains information on hazardous waste site assessment and remediation from 1983 to the present.
[8] SEMS is intended to provide repositories of, or access to, a variety of program data, including many key Superfund records.
[9] OAS is a comprehensive deployment platform designed to streamline application deployment by leveraging a single security, directory, and product metadata framework for all applications.

GAO Recommendation:
7. Strengthen and enforce password settings on Oracle database systems.

EPA Response:
The EPA concurs with the recommendation. The EPA implemented additional Oracle password controls including removing any default\weak passwords, limiting failed logon attempts, and enabling password life and verify functions. All users' profiles now have a password validation function attached, enforcing password complexity and an expiration period, enforcing password lifetime. Additional restrictions now enforced prevent password reuse and lock the account after a specified number of failed login attempts.

The replacement application (CIS) and new Oracle 11g backend will have enhanced security measures in place which will address these deficiencies. Oracle 11g will be able to mediate user access to data via their assigned authorities and labels, allowing data separation by sensitivity within single databases.

CBITS was designated to be decommissioned in September 2012. Additional CIS developments delayed the system deployment. CIS will be put into production in March 2013 with CBITS full decommission by 3rd quarter, FY 2013.

Database Remote Log-in -EPA did not fully control remote login access by system administrators logging in remotely to its Oracle database systems. NIST guidance and agency policy state that information systems should uniquely identify and authenticate users (or processes on behalf of users). However, remote login access by system administrators was not fully controlled on EPA database systems using Oracle, specifically, the CBITS, CDX, e-GGRT, CERCLIS, SEMS, and OAS/OCS applications. Remote users could directly authenticate into the database using the powerful INTERNAL account, or using SYSDBA and SYSOPER modes. As a result, increased risk exists that unauthorized users could gain access to these databases since access can occur outside of secure terminal service connections.

GAO Recommendation:
8. Provide controls to ensure remote access to Oracle database systems are appropriately restricted.

EPA Response:
The EPA concurs with the recommendation and has corrected the weakness. The replacement application (CIS) and new Oracle 11g backend will have enhanced security measures in place which will address these deficiencies. Oracle 11g will be able to mediate user access to data via their assigned authorities and labels, allowing data separation by sensitivity within single databases.

CBITS was designated to be decommissioned in September 2012. Additional CIS developments delayed the system deployment. CIS will be put into production in March 2013 with CBITS full decommission by 3rd quarter FY, 2013.

The internal connection is now only available to users directly logged into the server as the oracle user. Sys/System passwords are changed every 90 days, password complexity is enforced, reuse of old passwords is not allowed by database restriction, and the passwords are not shared with the user community.

MS SQL Server Database Accounts and Passwords - EPA did not adequately implement account and password controls for its VCenter VMWare MS SQL server database system, which supports system administrators of its VMWare ESXi environment10[10]in configuring virtual machines to deploy EPA business applications. NIST guidance and agency policy state that agencies should uniquely identify and authenticate users and provide strong password management controls. However, EPA did not always adequately implement account and password controls for its VCenter VMWare MS SQL server database system in support of configuring virtual machines in its VMWare ESXi environment, as shown here.

- Password expiration policy had not been applied to a system administrator account and two system SQL login accounts with administrator privileges.
- Strong password policy had not been applied to an account with administrator privileges (System administrator account).
- A guest account was enabled for the SQL MSDB database. The MSDB database is used by SQL servers for scheduling notifications/alerts and jobs such as backups, replication, and log shipping.
- The default BUILTIN Administrator SQL login account exists, which allows any account in the Windows Local Administrators group to also have SQL server system administrator rights.

As a result, there is a heightened risk that unauthorized individuals could exploit these vulnerabilities to gain unauthorized access to EPA systems.

GAO Recommendations:
9. Strengthen and enforce password settings for system administrator accounts, including SQL login accounts with administrator privileges on the VCenter VMWare MS SQL server database system.
10. Disable the guest account on the SQL database.
11. Remove the default BUILTIN Administrator SQL login account on the VCenter VMWare MS SQL server database system.

EPA Response:
The EPA concurs with the recommendations and has corrected the weaknesses as follows.

- Recommendation 9 - The EPA has strengthened the passwords for the "SA" login and service accounts to comply with password complexity standards. All of the other sysadmin logins are Windows AD logins, so they already comply with the standards.
- Recommendation 10 - The guest account is disabled on SQL Server instances.
- Recommendation 11 - The default BUILTIN\Administrator login was removed.

Routing Protocol Authentication - EPA did not always ensure that authenticated routing protocols were used on all of its Cisco network devices. NIST guidance states that information systems should identify and authenticate specific devices before establishing a connection. Additionally, National Security Agency (NSA) guidance states that organizations should configure security settings on Cisco routers and switches to provide for router authentication to prevent a router from accepting and employing unauthorized, malicious, or corrupted routing updates that would compromise the security or availability of the network. However, EPA did not authenticate the Enhanced Interior Gateway Routing Protocol[11] or Open Shortest Path First on all of its internal network devices. Additionally, EPA's vendor

[10] The VMWare ESXi environment via ESXi host servers provides the platform on which virtual machines reside.
[11] Enhanced Interior Gateway Routing Protocol is a Cisco proprietary advanced distance-vector routing protocol, with optimizations to minimize the routing instability incurred after topology changes. Routers that support it will automatically redistribute route information to routing neighbors.

providing Multiprotocol Label Switching[12] WAN communications did not authenticate the Border Gateway Protocol to its customer edge routers located onsite at EPA. Finally, EPA and its vendor providing the Managed Trusted Internet Protocol Service (MTIPS)[13] did not authenticate the Border Gateway Protocol between each organization's border routers. As a result, an incorrect route could be injected into EPA and its vendor routing tables, intentionally or unintentionally, potentially degrading the availability of the network.

GAO Recommendation:
12. Implement authenticated routing on all EPA Cisco network devices, including vendor devices providing WAN support to EPA.

EPA Response:
The EPA concurs with the recommendation and has addressed this issue by implementing MD5 level authentication for all routing protocols across OEI/OTOP/NCC managed devices. Also, the EPA implemented BGP from OEI/OTOP/NCC's internal devices to AT&T customer edge routers. The EPA will implement authenticated routing on Headquarters Cisco switches, and a plan of action and milestones will be established for this action.

Network Time Protocol Authentication on Network Devices - EPA did not use the Network Time Protocol authentication on all of its network devices. This protocol enables devices to maintain accurate time when synchronized to a trusted and reliable time server. NSA recommends that protocols be authenticated to prevent accidental or malicious changes to system clocks. Industry best practices recommend that protocols be authenticated to reduce the chance that an attacker can spoof the device's trusted time server and alter its system clock. However, EPA had not configured Network Time Protocol for networking devices to provide authentication. Consequently, EPA had diminished assurance that time stamps of facility access systems and security logs were accurate.

GAO Recommendation:
13. Configure the Network Time Protocol feature on all EPA network devices.

EPA Response:
The EPA concurs with the recommendation. On June 6, 2012 NSOC enabled NTP authentication to be used between all networking devices in the OEI/OTOP/NCC. This change enabled NTP peering and authentication between all network devices. This change was captured under CRQ#6182. The EPA has verified all Windows servers nationwide are operating on Domain Time Synchronization via Active Directory. Other Headquarters devices (e.g. VOIP, UNIX/LINUX, switches) will be checked to synchronize with National Bureau of Standards network clock, and a plan of action and milestones will be established for this action.

Remote Internet Access to E-Mail - EPA's e-mail system does not provide adequate authentication in providing remote Internet access to it. NIST guidance states that information systems should protect passwords from unauthorized disclosure and modification using a two-factor authentication: when stored and transmitted, and by establishing a trusted communication path between the user and the

[12] Multiprotocol Label Switching is a mechanism in high-performance telecommunications networks that directs data from one network node to the next based on short path labels rather than long network addresses, avoiding complex lookups in a routing table.
[13] MTIPS was developed by the General Services Administration to allow federal agencies to physically and logically connect to the public Internet and other external connections in compliance with OMB's Trusted Internet Connection initiative.

information system. However, two externally accessible websites that provide remote Hypertext Transfer Protocol Secure access to e-mail did not require two-factor authentication. As a result, EPA's network was at an increased risk of compromise.

GAO Recommendation:
14. Require two-factor authentication for remote Internet access to e-mail.

EPA Response:
The EPA concurs with the recommendation and has created a plan of action and milestones for remediation; the plan of action and milestone number is 120265. This remediation will be completed when EPA moves to Cloud email, scheduled to be completed by March 31, 2013.

Storage Area Network Switches User Account Management - EPA did not effectively manage user accounts on its Storage Area Network (SAN) switches. NIST guidance states that centralized password management helps organizations reduce the number of account identifiers and passwords that users need to remember. Moreover, NIST guidance and agency policy state that account and password policies should be established for information systems, including establishing minimum password complexity requirements, account lockout, and password minimum and maximum lifetime restrictions. However, centralized authentication was not applied for managing user accounts on SAN switches, and local user accounts on the switches were not controlled with password policies that included an account lockout control. Consequently, the switches were vulnerable to compromise and brute force password attacks.

GAO Recommendations:
15. Use centralized authentication in managing user accounts on SAN switches.
16. Apply password policy and account lockout controls to user accounts on SAN switches.

EPA Response:
The EPA concurs with the recommendations. A RADIUS Appliance software is being researched that can be used to manage access limitations on the network environment.

Network Device Remote Administration - EPA used a default password to remotely access and administer a router used for establishing a site-to-site virtual private network (VPN) in connecting contractors to its production network. NIST guidance and agency policy state that easily guessed default passwords should not be used for access to information systems. However, a default Cisco line password was used for remote administration into EPA's virtual private network router that connects contractors to its production network. As a result, remote administration into the VPN router is limited and highly susceptible to compromise.

GAO Recommendation:
17. Change the default password on the router used for establishing a site-to-site VPN in connecting contractors to EPA's production network.

EPA Response:
The EPA concurs with the recommendation and has corrected the weakness. The EPA made the following changes to address the finding on NCC-NSOC-VPN: (1) enabled password encryption; (2) enabled encryption of VPN pre-shared keys; (3) changed the default password; (4) added account of last

resort; (5) corrected Access Control Lists; (6) disabled Telnet and HTTP services; added welcome banner ; added AAA authentication; and upgraded IOS to FIPS 140-2 approved encryption standards.

AUTHORIZATION

Excessive Unix File Permissions - EPA did not always adequately restrict access to system files. NIST guidance states that privileges granted to user accounts should include only those privileges required for the users to perform their job functions. However, EPA's Linux-based intrusion-prevention servers provided world writeable access to system files. This level of access is inappropriate for all users and unnecessarily exposes the servers to compromise that could render them non-operational or limit their capability to function as intended.

GAO Recommendation:
18. Remove world-writeable access to EPA's Linux-based intrusion-prevention servers' system files.

EPA Response:
The EPA concurs with the recommendation and has corrected the weakness. The EPA decommissioned all affected IDS systems identified in this finding once new UTM Firewalls were implemented on September 8, 2012.

User Account Management - EPA had an excessively large number of inactive accounts across its network domains. NIST guidance states that unneeded user accounts should be disabled. Moreover, agency policy states that managers/supervisors must provide immediate notification to designated support systems and applications administrative personnel when an agency employee or contractor no longer requires access and managers should review access logs to identify and delete dormant accounts (those not used for 30 days), as appropriate. However, many non-disabled accounts applicable to the EPA CBITS[14] local area network, CDX,[15] Demilitarized Zone Active Directory (DMZ AD), and intranet domains were never used or never logged into for 90 days or longer, as illustrated here in examples of user accounts not being locked or disabled:[16]

EPA Intranet domain (52,507 accounts)
- More than 9,400 accounts created but never used
- More than 700 accounts with a last logon in 2008
- More than 3,400 accounts with a last logon in 2009
- More than 3,400 accounts with a last logon in 2010
- More than 1,700 accounts with a last logon occurring on or before May 31, 2011

CDX domain (81 accounts)
- 37 created but never used

[14] Original CBI export notices are maintained in the CBI center and are tracked using CBITS. The CBI center is responsible for maintaining the official CBI export notice records. Information on the CBI notices submitted to EPA is kept in a log book. This information includes the CBI document control number, the name of the chemical exported, the country of import, and the date the export notification letter was sent to the foreign government.
[15] CDX is the point of entry on the Environmental Information Exchange network for environmental data exchanges for the agency. CDX enables EPA and participating program offices to work with stakeholders–including state, tribal, and local governments and regulated industries–to enable streamlined, electronic submission of data via the Internet.
[16] Based on GAO analysis of user account management records reported as of January 11, 2012.

DMZ AD domain (82 accounts)

- 52 created but never used

CBI local area network domain (838 users)

- 120 accounts created but never used
- 41 accounts with a last logon occurring on or before September 29, 2011

Additionally, complete account logon information was not available for many of the domain controllers reviewed, which indicates that many more non-disabled accounts that were not identified could also be inactive or never used. As a result, there is an increased risk that a significant number of EPA user accounts across major domains not reviewed could be vulnerable to malicious use.

GAO Recommendation:
19. Disable or delete all EPA intranet, CDX, DMZ AD, and CBI local area network domains' user accounts that are unused or that have been inactive for more than 90 days.

EPA Response:
The EPA concurs with the recommendation.

- For CDX a Plan Of Actions & Milestones is scheduled to delete domain user accounts that are unused or inactive in excess of 90 days by the end of July 2012.
- For CBI LAN the inactive and dormant user accounts will be disabled from the CBI LAN. An audit script program will be enabled to verify that accounts have been disabled and/or deleted. CBI LAN account management procedures will be revised to comply with NIST and FISMA security requirements.
- For Intranet and DMZ AD appropriate actions have been completed.
- The CDX and CBI support teams have been notified of items identified in the report which are accounts that were created and never used: CDX, DMZ and CBI will be responsible for removing unnecessary accounts per this report by January 31, 2013. Regarding the EPA Intranet Domain Accounts, some of these accounts are not only user accounts but are service accounts. The user accounts that are no longer active or have not logged in during the time period per the NIST guidelines will be disabled/deleted. This action will be completed by January 31, 2013.

Wireless Access Control Server Access Restrictions - EPA did not effectively limit access to its Cisco wireless access control server. The purpose of the access control server is to manage access to EPA headquarters' wireless networks, which includes establishing wireless network encrypted sessions and enabling wireless users' authentication to EPA's Active Directory. NSA guidance recommends creating a set of filtering rules that permit and prohibit certain traffic from accessing network devices. However, EPA did not use the Cisco wireless access control server Internet Protocol (IP) address filtering option to regulate traffic to the device. Moreover, the access control server can be reached from any source, as we found out by accessing the device from the Research Triangle Park library. As a result, the Cisco access control server is unnecessarily susceptible to unauthorized access attempts from any source.

GAO Recommendation:
20. Apply the IP address filtering option to restrict access to EPA's Cisco wireless access control server.

EPA Response:
The EPA concurs with the recommendation and has corrected the weakness. All security concerns regarding Wireless Access Control Server Password policy have been addressed by OEI/EDSD Wireless team. All Policies are created off of NIST standards and DoD STIG guidelines and recommendations, as well as industry standards.

Windows Account Enumeration - EPA did not always prohibit anonymous enumeration of user account names on its Windows systems. NIST guidance states that information systems should uniquely identify and authenticate users (or processes on behalf of users). However, two CBI domain controllers, two servers, and an administrator workstation were not configured for adequate identification and authentication by allowing anonymous logins of users (also known as null session connections). Additionally, a CDX domain controller and two servers (authentication and web), and a CBITS domain controller and server (input Accel) allowed the logon to the Windows dialog box to display the name of the last user to logon to the computer. As a result, an unauthorized user could anonymously list account names and use the information to perform social engineering attacks or attempt to guess passwords. Moreover, an unauthorized user with physical or remote terminal access could view the name of the last user who logged onto the server and then try to guess the password, use a dictionary, or use a brute-force attack to try to logon.

GAO Recommendation:
21. Configure network access to not allow anonymous enumeration of Windows user accounts.

EPA Response:
The EPA concurs with the recommendation. A Group Policy has been implemented on domain to disable the NULL session

Remote Root Login - EPA system owners did not always adequately protect the root account on a Linux server. NSA network security guidance recommends prohibiting the root account user from logging directly into a remote system through proper configuration in files. However, EPA system owners allowed remote root logins to a jump server (Stargate) used to access National Computer Center (NCC) network infrastructure devices. Allowing direct remote root logons increases the risk of a host compromise and reduces accountability for user actions, since root is by design a shared account.

GAO Recommendation:
22. Prevent direct remote root logon to the EPA Linux server cited.

EPA Response:
The EPA concurs with the recommendation and has corrected the weakness. The EPA disabled direct root login on the affected system.

Source Routing - EPA did not always disable source routing. NSA guidance states that IP source routing should be disabled. However, IP source routing was enabled on 56 network devices. Source routing is a technique whereby the sender of a packet can specify the route that a packet should take through the network. Source routing can be used for hacking, since it allows an attacker to reach a sensitive server by directing packets to reach that server. As a result, an attacker could bypass access controls and routing tables to view sensitive data transmitted on the network, including unencrypted passwords for critical systems.

GAO Recommendation:
23. Disable source routing on the 56 network devices.

EPA Response:
The EPA concurs with this recommendation and has corrected the weakness. The Group Policy that was implemented on domain to disable the NULL session resolved this issue. On May 23, 2012 the EPA disabled IP Source Routing on the OEI/OTOP/NCC managed devices.

Database Remote Access - EPA's CDX production database system does not adequately prevent remote access by database users. NIST guidance and agency policy state that users' access should be appropriately restricted based on least privilege and need-to-know principles. However, the CDX production database, through an enabled Oracle-supplied global utility (utl_file_dir), allowed any database user on any client server to remotely read or write to any directory that the owner of the Oracle software had rights to access. This level of access by any user leaves this system highly vulnerable to compromise by escalating privileges to the system level.

GAO Recommendation:
24. Disable the use of the Oracle-supplied global file access utility on the CDX production database system.

EPA Response:
The EPA concurs with this recommendation. The Oracle-supplied global file access utility (utl_file_dir) was disabled during the first week of July 2012. The CDX production database now uses a CREATE directory, which is safer than the UTL file, and appropriately restricts based on least privilege and need-to-know principles.

Oracle Database Privileges and Roles - EPA did not always adequately restrict access to sensitive database system privileges and roles. NIST guidance and agency policy state that a user should be granted only the access and rights to information and information systems that are needed to perform the functions of the job. However, sensitive system privileges and roles applicable to database administration were not always adequately restricted, as illustrated in these examples:

- Public roles were granted to execute permissions to sensitive Oracle database administration functions, referred to as packages, for EPA database systems supporting CBITS, CDX, eGGRT, CERCLIS, SEMS, and OAS/OCS applications.
- The CBITS database system data dictionary was accessible with any level of privilege.
- An SQL security parameter (SQL92) was not enabled for databases supporting CBITS, CDX, and OAS/OCS applications that required a user to have the select privilege on a table in order to be able to execute "update" and "delete" statements on a given table.
- "Resource" roles in all EPA database systems reviewed had been granted highly sensitive system "create procedure" privileges. Moreover, "connect" roles in EPA's CBITS database had been granted highly sensitive system "create" privileges. Oracle recommends revoking these privileges from the roles and providing for these privileges in newly-defined roles for database administrator use only.

As a result of these weaknesses, there is heightened risk that the database systems could be compromised through privileged escalation, execution of arbitrary commands via scripts, denial of

service, or unauthorized access where sensitive system files can be modified and sensitive information disclosed via SQL-injected queries.

GAO Recommendations:
25. Remove sensitive privileges and roles related to Oracle database administration functions from general application users.
26. Restrict access to the CBITS database system data dictionary to only those access levels needed to perform functions of the job.
27. Enable the SQL security parameter, SQL92.
28. Revoke system privileges from the "resource" and "connect" roles, and redefine system privileges from the "resource" and "connect" roles to newly created roles for database administrator use only.

EPA Response:
The EPA concurs with the recommendations and has corrected the weaknesses as follows:

- Recommendation 25 - User role restrictions have been strengthened. Resource role is now restricted to users who require it (i.e. schema owners and TCs) for day to day functions. The replacement application (CIS) and new Oracle 11g backend will have enhanced security measures in place which will address these deficiencies. Oracle 11g will define roles and responsibilities for all CIS users. The SysAdmin and SysDBA will be the designated system managers with the appropriate access rights for the CIS Oracle administration functions.
- Recommendation 26 - The replacement application (CIS) and new Oracle 11g backend will have enhanced security measures in place which will address these deficiencies. Oracle 11g will define roles and responsibilities for all CIS users. The SysAdmin and SysDBA will be the designated system managers with the appropriate access rights for the CIS Oracle administration functions.
- Recommendation 27 - Oracle separates the insert, update, delete, and select permissions into separate privileges. Having select privilege does not grant permission to alter the data in any way. The SQL92 option is not currently enabled as enabling it would actually reduce the security in the databases. Developers often have programs update audit tables in the database where they do not wish the users to see the contents. With the current setting of SQL92, this is possible. Enabling SQL92 would force developers to give users select permissions on such audit tables, allowing them to see the content.
- Recommendation 28 - Resource role is now restricted to schema owners and administrators. The connect role has been reduced to be a synonym for "create session" only. We are working through replacing the resource role with a renamed role to remove it from the public namespace.

MS SQL Extended Stored Procedures - EPA did not have adequate restrictions on sensitive MS SQL extended stored procedures[17] on its VCenter VMWare MS SQL server database system used in support of centrally managing ESXi servers. NIST guidance and agency policy state that users should be granted only the access and rights to information and information systems that are needed to perform the functions of their jobs. However, EPA did not have adequate restrictions on MS SQL extended stored procedures, as illustrated in the following examples:

- Several extended stored procedures inappropriately allowed interaction with the system registry using the privileges of the account that the SQL server was running (normally SYSTEM versus restricted to system administrator). These procedures included xp_regaddmultistring,

[17] An extended stored procedure is a way to extend the capabilities of Transact-SQL (T-SQL) to include any resources or services available to Microsoft Win32 system applications.

xp_regdeletekey, xp_regdeletevalue, xp_regenumvalues, xp_regremovemultistring, and xp_regwrite.

- Sensitive extended stored procedures were present that exposed sensitive functions to non-system administrators and could be easily accessed using T-SQL statements (e.g., xp_availablemedia, xp_dirtree, xp_enumerrorlogs, and xp_loginconfig).
- Sensitive SQL system registry-level stored procedures could be inappropriately executed through public role permissions on VCenter VMWare MS SQL server database system (xp_instance_regread and xp_regread).

As a result, heightened risk exists that the VCenter database could be compromised through elevated system privileges that could lead to compromise of the database system (e.g., unauthorized disclosure and use of password/hashes stored in the system registry).

GAO Recommendations:
29. Restrict access to extended stored procedures on the server database system to system administrators only.
30. Remove public role registry permissions to the system registry-level stored procedures on the VCenter VMWare MS SQL server database system.

EPA Response:
The EPA concurs with the recommendations and has corrected the weaknesses. The EPA completed this task as part of the SQL Server security overhaul. This review and overhaul was undertaken, in part, in response to the initial GAO audit. Many user permissions and security settings, especially those associated with the SA user level, were reviewed and revised as part of this review.

Network Device AAA Authorization - Many EPA network devices are not configured for the level of authorization necessary for central management control through EPA's TACACS+ central network management server. NSA guidance states that organizations should configure security settings on Cisco routers and switches to provide for use of the Authentication, Authorization, and Accounting (AAA) network security services.[18] However, EPA did not enable the AAA authorization feature on several network devices. Consequently, authorization in accessing and managing many network devices' configurations was not centrally controlled as intended through EPA's TACACS+ central network management server and could allow unauthorized access into the network.

GAO Recommendation:
31. Enable the use of AAA authorization on all Cisco network devices.

EPA Response:
The EPA concurs with the recommendation. On July 25, 2012, the EPA conducted a review of all managed devices and those identified not covered under TACACS were added and all passwords changed. Work was covered under CRQ #7664. In addition, the EPA will address the Headquarters TACACS corrective action to comply with the recommendation via a plan of action and milestone.

[18] AAA network security services provide the primary framework through which access control is set up on a router or access server. For example, AAA authorization works by assembling a set of attributes that describe what the user is authorized to perform. These attributes are compared to the information contained in a database for a given user and the result is returned to AAA to determine the user's actual capabilities and restrictions. The database can be located locally on the access server or router or it can be hosted remotely on a RADIUS or TACACS+ security server.

Access Control Lists - EPA did not always effectively limit access to many of its network devices. NSA guidance recommends creating a set of filtering rules, also known as access control lists that allow access to the traffic identified on the list and prohibit other traffic. However, EPA did not always define or apply access control lists to hosts or systems, as illustrated by the following examples:

- CBI network devices did not implement access control lists at the Office of Pollution Prevention and Toxics.
- EPA's router used to establish the contractor's VPN connectivity to EPA's production network did not apply access control lists.
- EPA did not configure its virtual teletype interfaces on many of its network devices with access control lists to limit access, including one device managed and owned by its vendor as part of its WAN implementation.
- Transmission Control Protocol wrappers for two Linux infrastructure support servers (Stargate and Defender) did not sufficiently restrict accounts seeking access to the servers where the file (host.deny) for restricting access to the servers was not defined.

GAO Recommendations:
32. Configure access control lists on the Office of Pollution Prevention and Toxics' CBI network devices to limit access.
33. Configure access control lists on the router connecting contractors to the EPA production network.
34. Configure virtual teletype interfaces with access control lists to limit access to network devices, including the network device managed and owned by its vendor as part of its WAN implementation.
35. Define the host.deny file to appropriately restrict user access to the two Linux-based infrastructure support servers.

EPA Response:
EPA concurs with the recommendations. A RADIUS Appliance software is being researched that can be used to manage access limitations on the network environment.

Recommendations 33-35, the EPA added TCP wrappers to explicitly allow and deny access to the identified jump boxes (ie Stargate). Defender was decommissioned as part of the Firewall UTM deployment on September 8, 2012.

Linux Security Policy - EPA did not always effectively implement adequate security on its Linux servers. NIST guidance states that organizations should configure security settings to the most restrictive mode consistent with operational requirements. This is accomplished in Linux by implementing Security-Enhanced Linux (SELinux). SELinux is an enhancement to the Linux kernel that implements mandatory access control and role-based access control. However, EPA had disabled SELinux security on three Linux servers that provide infrastructure support applicable to a jump server, syslog, and Domain Name Services (DNS). Consequently, the security capabilities of these servers to limit accesses of processes and objects based on least privilege concepts in confining damage caused by malicious or flawed applications are significantly diminished.

GAO Recommendation:
36. Enable SELinux or an alternative mandatory access control-based system on all Linux servers.

EPA Response:
The EPA concurs with the recommendation. Note: SELinux was enabled in permissive mode on VitalQIP appliances. Vendor does not support Restrictive mode as this may potentially cause

operational outage. Compensating controls are in place: (1) TCP wrappers restrict access to systems; (2) Security logs are sent to ArcSight for correlation and review; and (3) system administrator accounts are limited to two Network and Security Operations Center (NSOC) personnel.

User Account Removal - EPA did not remove active accounts in a timely manner for several employees who no longer needed it. EPA policies require that information resource access privileges shall be coordinated with staff personnel actions and that access authorizations for staff departing the agency must be promptly disabled. However, EPA did not remove or deactivate active network access for CBI local area network and CBITS accounts for separated employees. One of the individuals with the CBI local area network account separated in October 2011, yet still had an active account in January 2012. The other employee separated in August 2011 and had an active CBITS account in January 2012. As a result of not managing the accounts of separated employees, unauthorized users could access EPA systems and pose a risk to EPA's network.

GAO Recommendation:
37. Deactivate and remove accounts of separated employees with access to EPA's network immediately.

EPA Response:
The EPA concurs with the recommendation. The inactive user accounts will be disabled from the CBI LAN. An audit script program will be enabled to verify that accounts have been disabled and/or deleted. CBI LAN account management procedures will be revised to comply with NIST and FISMA security requirements.

CRYPTOGRAPHY

Virtual Private Network Split Tunneling - EPA had not fully configured its Firepass Secure Sockets Layer (SSL) VPN appliance to prevent the use of split tunneling. Split tunneling occurs when a client server on an external network is not configured to send all its traffic to the organization's gateway and could bypass a VPN tunnel. NIST guidance recommends that the use of split tunneling be prohibited. However, EPA had configured its Firepass SSL VPN appliance to permit the use of split tunneling for more than 140 contractors' user accounts that were not limited to the contractors' own network and to 41 EPA employees in the employee split tunnel group that were primarily serving as system administrators. Consequently, these users could bypass the gateway-level security to communicate directly and simultaneously with many of the organization's internal network subnets and another network (typically the Internet). If a user's workstation is compromised, a remote attacker could connect to the host surreptitiously and use its tunnel to gain unauthorized access to the EPA network.

GAO Recommendation:
38. Configure the Firepass SSL VPN appliance to disable or limit split tunneling to contractors based on operational needs and fully to the EPA employee split tunnel group.

EPA Response:
The EPA believes this item was resolved with GAO through discussions following the draft report.

Secure Shell Keys - EPA did not always encrypt SSH private keys stored on its Unix infrastructure servers. NIST states that authenticator content is to be protected from unauthorized disclosure and modification. However, SSH private keys on its Stargate and Snapper infrastructure support servers were stored without using encryption and passphrases features available in SSH. SSH key-based

authentication provides a mechanism to authenticate users based on the possession of the private key. Unencrypted storage gives anyone with read access to the file the ability to use the key without authorization. As a result, unauthorized users could access the private keys and masquerade as authorized users.

GAO Recommendation:
39. Encrypt Unix infrastructure servers' private keys used for SSH key-based authentication.

EPA Response:
The EPA concurs with the recommendation and has corrected the weakness. The EPA verified and removed all private keys that were not encrypted.

Network Device Encryption - EPA did not always apply encryption to its network devices. NIST guidance states that authenticator content is to be protected from unauthorized disclosure and modification, including passwords encrypted while stored and in transit. Moreover, agency policy states that information managers shall limit access to and encrypt files linking passwords and user IDs. However, four network devices (National Computer Center VPN, pyd-s4a1104, ncc-svr-s1, and nh1112), including the router contractors use to establish a site-to-site VPN connection[19] into EPA, had the service password encryption feature disabled, which encrypts all password types on Cisco network devices. Additionally, the pre-shared keys on the VPN router used to encrypt the site-to-site VPN connection were stored in clear text rather than in encrypted form. Without using encryption, passwords and pre-shared keys used in setting up a VPN connection are at increased risk of compromise.

GAO Recommendations:
40. Enable the service password encryption feature on Cisco network devices cited.
41. Encrypt the pre-shared keys stored on the VPN router.

EPA Response:
The EPA concurs with the recommendations and made the following changes to address the finding on NCC-NSOC-VPN: (1) enabled password encryption; (2) enabled encryption of VPN pre-shared keys; (3) changed the default password; (4) added account of last resort; (5) corrected Access Control Lists; (6) disabled Telnet and HTTP services; (7) added welcome banner; (8) added AAA authentication; and (9) upgraded IOS to FIPS 140-2 approved encryption standards. Other OEI/OTOP/NCC managed device was decommissioned as services were no longer required.

In addition, the EPA will work with GAO to obtain additional detail on the cited devices in order to take action on the service password encryption.

Network Devices' Encryption Algorithm - EPA did not always employ a robust encryption algorithm for its network devices. NSA and Cisco guidance recommend that passwords in Cisco network devices should use the Message Digest Algorithm 5 (MD5)20 [20]versus type 7 Cisco defined algorithm, which is known in the commercial security community to be weak. However, EPA network devices were using the "enable password"[21] with type 7 encryption without the "enable secret"[22] password. The "enable

[19] Site-to-site allows offices in multiple fixed locations to establish secure connections with each other over a public network such as the Internet.
[20] MD5 is a widely used cryptographic checksum algorithm.
[21] The "enable password" on Cisco network devices is used to set a local password to control access to various privilege levels and uses a weak encryption algorithm.

secret" command provides an additional layer of security (using the stronger MD5) for encrypting passwords. Additionally, many Cisco routers, including EPA's VPN router that connects contractors to its production network, in providing alternative fallback authentication into network devices (in the event that the standard TACACS+ server authentication fails), use the "line" password with type 7 encryption instead of the local username account database that uses the stronger MD5 algorithm. The password type 7encryption is very weak, can be cracked instantly, and is no longer recommended by Cisco.

As a result of using weak password algorithms, many devices were susceptible to unauthorized access from an attacker who could compromise privileged accounts using the weaker "line" password.

GAO Recommendations:
42. Use the "enable secret" password feature to provide an additional layer of security over the "enable password" feature.
43. Discontinue use of the "line" password with type 7 encryption and instead use the local username database with MD5 encryption of passwords.

EPA Response:
The EPA concurs with the recommendations. The EPA conducted a review of all managed devices and implemented the following steps: (1) enable secret password was implemented where deficient; and (2) line password with type 7 has been removed and replaced with TACACS authentication.

Insecure Network Protocols - EPA allowed the use of insecure network protocols for managing its IT infrastructure and operations. NIST guidance states that organizations should use secure protocols that can provide encryption of both passwords and data and that can replace less secure protocols (e.g., Telnet, Trivial File Transfer Protocol, and File Transfer Protocol) unless absolutely required and tunneled over an encrypted protocol. However, EPA used insecure protocols, including Telnet for remote administration, Trivial File Transfer Protocol for network management, and File Transfer Protocol for file transfers. All data were being transmitted in clear text, and the three protocols do not have authentication mechanisms to verify whether the user has reached a valid destination, as illustrated in the following examples:

- EPA permitted the use of Telnet, Trivial File Transfer Protocol, and File Transfer Protocol, for example, in providing contractors' and a federal agency's connectivity into EPA's internal network (NE and AGF), a firewall in the DMZ allowing a Telnet connection for network management, and another firewall setup with temporary rules created to support deployment of the CBI local area environment in March 2010.
- Remote administration of network devices include the use of Telnet, Trivial File Transfer Protocol, and File Transfer Protocol, which exposes devices to compromise such as Dynamic Host Configuration Protocol data backed up from a switch containing sensitive IP address and networking information associated with its host that could be retrieved by an attacker in targeting systems to exploit.
- Telnet is used by two management console servers for out-of-band management of network devices.

[22] The "enable secret" command is used to set the password that grants privileged administrative access to the Cisco IOS system. The "enable secret" command should be used rather than the older "enable password" command because it uses a stronger encryption algorithm.

- Unix application and infrastructure support servers include use of Telnet, as well as the Network File System, which is an unencrypted protocol that allows a user on a client computer to access files over a network in a manner similar to how local storage is accessed.

As a result, sensitive data from the use of these protocols were unnecessarily exposed to inappropriate disclosure and possible compromise of EPA systems.

GAO Recommendations:
44. Configure firewalls to prevent the use of Telnet, Trivial File Transfer Protocol, and File Transfer Protocol to and from untrusted networks.
45. Discontinue the use of Telnet, Trivial File Transfer Protocol, and File Transfer Protocol for remote administration of network devices.
46. Disable the use of Telnet for out-of-band management of network devices by the cited console servers.
47. Discontinue the use of Telnet, File Transfer Protocol, and Network File System on Unix application and infrastructure support servers.

EPA Response:
The EPA concurs with the recommendations. In response to the network-related recommendations, the EPA conducted a review of all managed devices and removed use of Telnet, FTP and TFTP where identified as non-mission essential. TFTP is being used for a specified amount of routers in order to transfer DHCP databases to the IPAM. Currently Cisco does not support SCP transfers for this purpose. EPA has applied compensating controls such as traffic being limited internal to the network only.

In response to the application hosting related recommendations, the EPA is phasing out the use of Telnet, File Transfer Protocol, and Network File System on Unix application and infrastructure support servers, but they are currently still required by our customer base. The EPA has created a plan of action and milestones for remediation of this issue.

Solaris Password Encryption - EPA did not always properly encrypt Solaris passwords. NIST requires an encryption algorithm that complies with Federal Information Processing Standard (FIPS) 140-2. However, EPA used the non-FIPS-compliant "crypt" algorithm for Solaris password hashing on three infrastructure support servers (Cerberus, Snapper, and Tortoise). As a result, a malicious user who is able to obtain access to the password file could exploit this weakness to obtain user passwords and gain access to sensitive systems.

GAO Recommendation:
48. Implement a FIPS-compliant encryption algorithm for Solaris password hashing.

EPA Response:
The EPA concurs with the recommendation. Systems are scheduled for decommissioning.

Note: Current systems are EOL and the Solaris version in use does not support FIPS compliant algorithms. Systems are scheduled for replacement in accordance with the NSOC Log Consolidation Plan. The EPA added the following compensating controls: (1) TCP wrappers to explicitly allow and deny access to the identified systems; (2) Cerberus resides on a limited access security VLAN with restrictive ACLs applied; (3) system administrator accounts are restricted to NSOC personnel; and (4) two factor authentication is required on all systems.

Wireless Encryption - EPA allowed the use of (1) multiple authentication modes that were not in accordance with EPA policy on its wireless networks and (2) wireless controllers that are not FIPS-mode enabled (i.e., fully compliant with FIPS 140-2 requirements). NIST guidance recommends and EPA's policy calls for use of the Extensible Authentication Protocol–Transport Layer Service (EAP-TLS) for user workstations to authenticate during the connection process to an organization's enterprise wireless network. The protocol requires strong mutual cryptographic authentication of workstations to the authentication server (both the user's workstation and authentication server must have a certificate).[23] Additionally, NIST guidance recommends that FIPS mode be enabled on wireless controllers,[24] which restricts the use of less secure encryption algorithms. However, EPA allowed use of non-TLS based solutions for authenticating wireless workstations to EPA's enterprise wireless networks, and its wireless controllers were not FIPS mode enabled. As a result, heightened risks exists that wireless workstations can be compromised because they may not be effectively authenticated to EPA's wireless networks with confidentiality and integrity checks in accordance with policy, and weak/less secure encryption algorithms could be used in wireless controllers. Moreover, risk is further heightened since compromised wireless networks would have access to EPA's infrastructure, including the TACACS+ servers.

GAO Recommendations:
49. Use EAP-TLS for authenticating EPA's wireless workstations to the agency's enterprise wireless networks.
50. Enable FIPS mode on EPA's wireless controllers.

EPA Response:
The EPA concurs with the recommendations. The EPA currently uses EAP-TLS for authenticating wireless LANs. The EPA will close down all non-EPA-TLS authentication policies in its ACS servers. A POA&M will be established.

Secure HTTPS Protocol - The secure Hypertext Transfer Protocol for requesting changes to MTIPS[25] connection services was not used on the access provider's web portal. NIST guidance states that organizations should use encryption to protect the confidentiality of remote access sessions. However, we observed that the vendor's web portal, which was used by EPA to request changes to its MTIPS access provider's managed firewall, did not use the Hypertext Transfer Protocol Secure. As a result, communication through the vendor's web portal, including credentials for authenticating onto the portal, is in clear text and therefore more likely to be disclosed to unauthorized individuals.

GAO Recommendation:
51. Enable secure Hypertext Transfer Protocol to encrypt Hypertext Transfer Protocol traffic on the vendor's web portal.

---

[23] Mutual TLS authentication is generally more secure than one-way TLS authentication coupled with one or more additional EAP methods. Certificates, along with usernames, are verified during EAP-TLS authentication by the access control server prior to clients being granted access to the wide local area network.
[24] Wireless controllers establish wide local area network connections with access points in managing voice/video/data traffic.
[25] The MTIPS program provides TIC-compliant managed security services through Networx. Networx offers managed security services through the MTIPS program, which complies with the TIC initiative.

EPA Response:
The EPA concurs with the recommendation and has corrected the weakness. The EPA coordinated with AT&T to address this issue. AT&T portals are now HTTPS enabled.

Database Password Encryption - EPA's encrypted passwords were using a weak cryptographic algorithm that was not compliant with FIPS 140-2 and could not be patched. These passwords were for administrative system accounts in a number of files in Oracle database operating systems related to the CBITS database and a database providing support to EPA's Oracle Application Server application. NIST guidance states that passwords should be encrypted in storage and in transmission using a cryptographic algorithm that is FIPS 140-2 compliant. However, a number of logfiles in the database operating systems cited contained weakly encrypted passwords that cannot be patched (i.e., upgraded to a FIPS compliant algorithm) for sensitive SYS, SYSTEM, SYSMAN, and DBSNMP accounts. As a result, the database systems were susceptible to unauthorized access from an attacker compromising database accounts.

GAO Recommendation:
52. Remove or secure the Oracle logfiles if they cannot be removed.

EPA Response:
The EPA concurs with the recommendation. The replacement application (CIS) and new Oracle 11g backend will have enhanced security measures in place which will address these deficiencies.

Database Link System Access - EPA did not adequately encrypt system access to its CBITS database system when connecting to other Oracle servers through database links. NIST guidance states that organizations should encrypt sessions between host systems. In addition, Oracle states that database links should use encrypted passwords. However, the CBITS database link did not encrypt passwords. As a result, CBITS database links were highly vulnerable to compromise.

GAO Recommendation:
53. Encrypt database link passwords for the CBITS database system.

EPA Response:
The EPA concurs with the recommendation. The replacement application (CIS) and new Oracle 11g backend will have enhanced security measures in place which will address these deficiencies.

Router Message Integrity - EPA did not protect the message integrity of a Cisco redundancy protocol used on its enterprise network devices. NIST guidance states that information systems should protect the integrity of transmitted information by using cryptographic mechanisms that recognize changes to information during transmission. However, EPA did not apply MD5 for authentication to protect the message integrity of the Hot Standby Router Protocol[26] that was used to implement redundancy between router network devices including default gateway routers. As a result, anyone on the network could monitor a multicast Hot Standby Router Protocol message packet and compromise the agency's network by crafting a packet that pretended to have a higher priority and allow a malicious user to become the

[26] The Hot Standby Router Protocol provides a mechanism that is designed to support non-disruptive failover of IP traffic in certain circumstances. In particular, the protocol protects against the failure of the first hop router when the source host cannot learn the IP address of the first hop router dynamically.

new active router. We demonstrated this by capturing Hot Standby Router Protocol messages through a network sniffer run in a public area network located in the Research Triangle Park library.

GAO Recommendation:
54. Configure the Hot Standby Router Protocol with MD5 algorithm authentication.

EPA Response:
The EPA concurs with the recommendation and is remediating the weakness. On 12/8/2012 the EPA completed the implementation of HSRP with MD5 encryption on OEI/OTOP/NCC managed devices.

Windows Password Protection - EPA did not enforce sufficiently strong password protection. NIST guidance states that information systems should protect passwords from unauthorized disclosure and modification when stored and transmitted and passwords should be encrypted with a one-way hash function to ensure that the computations used in a dictionary or password cracking attack against a stolen password file cannot be used against similar password files. NSA guidance also recommends protecting passwords and advises against the use of the Windows LAN Manager setting,[27] a weak password algorithm that can be easily compromised. Further, according to the vendor, use of the NT LAN Manager version 2 authentication level is strongly recommended to resolve these issues. However, EPA Windows systems were not always sufficiently configured to protect passwords. Specifically, an administrator workstation and Office of Pollution Prevention and Toxics domain controller had the LAN Manager setting enabled. Additionally, two CERCLIS Citrix servers, a Clean Air Markets Division Business System (CAMDBS) server and a SEMS staging application web server had the NT LAN Manager Only response setting enabled, which did not provide for a secure channel to protect the authentication process.[28] As a result, a malicious user could exploit these weaknesses to obtain user passwords and gain access to sensitive EPA servers.

GAO Recommendation:
55. Configure NT LAN Manager Version 2 authentication on EPA Windows-based systems.

EPA Response:
The EPA concurs with the recommendation. Settings have been implemented accordingly and OEI/OTOP/NCC's Windows systems have been properly configured to protect passwords by disabling NT LAN Manager or by properly configuring NT LAN Manager version 2 authentication.

Windows Terminal Services' Connection - EPA did not configure two Windows-based jump servers on its internal network to fully prevent insecure connections. NIST guidance states that information systems should establish a secure connection between the user and the information system, which includes use of a FIPS-validated cryptographic mechanism to protect the confidentiality and integrity of transmitted information. However, two jump servers were not set to authenticate prior to establishing the connection (certificates set to "none"), which renders encryption ineffective for internal connections. As a result, EPA systems using these services were susceptible to compromise, such as from man-in-the-middle attacks.

[27] LAN Manager converts passwords to all uppercase characters, creating even weaker passwords. Because of the limited complexity, any eight-character NT LAN Manager password can be cracked in an extremely short period of time.
[28] The NT LAN Manager protocol was the default for network authentication in the Windows NT 4.0 operating system. It is retained in Windows 2003 for compatibility with down-level clients and servers.

GAO Recommendation:
56. Enable authentication on the two Windows servers cited prior to establishing the Windows terminal services connection.

EPA Response:
The EPA concurs with the recommendation and has corrected the weakness. The EPA corrected this deficiency by implementing SSL encryption for Rook & Knight (Jump boxes in question).

AUDIT AND MONITORING

Network Device Audit Logs - EPA did not have effective audit logs for its network devices. NIST guidance states that organizations should retain sufficient audit logs to provide support for after-the-fact investigation of security incidents. This includes centralized review and analysis of audit log records through logging servers that receive log data from host systems that generate the data. However, EPA did not have effective audit logs, as illustrated in the following examples:

- At least 13 network devices did not have remote logging configured.
- More than 150 network devices had remote logging set to a severity level not sufficient to log important security information such as access control list permit/deny matches, login attempts successful and failed, configuration changes, and port tampering.
- The Cisco wireless access control server at headquarters did not have remote logging configured.

As a result, EPA did not have the information needed to enable sufficient audit and monitoring of security-related events.

GAO Recommendation:
57. Enable remote logging on all devices reviewed and at a severity level sufficient to capture important security information.

EPA Response:
The EPA concurs with the recommendation and will work to develop a procedure and schedule updates to IOS, Firmware, Patches – as we do not want to cause a connectivity issue internally or with the Agency WAN. The EPA will also work with GAO to clarify the examples cited and to identify the 13 network devices that did not have remote logging configured and the 150 network devices that had remote logging set to too low a severity level.

Windows Host-Based System Auditing - EPA did not always adequately provide for auditing of Windows host-based systems' security-related events. NIST guidance states that organizations should enable and retain sufficient audit logs to allow monitoring of key activities and provide support for after-the-fact investigations of security incidents. However, EPA did not have auditing enabled on its CDX production domain controller that provides support for receiving sensitive confidential business information from commercial entities. As a result, EPA was not able to monitor key activities on this production domain controller.

GAO Recommendation:
58. Enable auditing on the CDX production domain controller.

EPA Response:
The EPA concurs with the recommendation and has corrected the weakness. The EPA has enabled auditing on the CDX production domain controller.

MS SQL Database Logging - EPA did not set the number of logs to a sufficient level to prevent the logs from being overwritten on its VCenter VMware MS SQL server database system used in support of centrally managing ESXi servers for configuring virtual machines that deploy most of EPA's applications. NIST and agency policy state that sufficient audit logs should be continuously maintained to allow timely monitoring of key user activities. However, the number of error logs retained on the VCenter VMware MS SQL server database system was seven before the oldest log was overwritten. As a result, log information may not be available to effectively monitor and investigate security-related events and incidents.

GAO Recommendation:
59. Set the number of logs retained to a sufficient level to prevent logs from being overwritten.

EPA Response:
The EPA concurs with the recommendation and has corrected the weakness. The number of logs is set to ensure log files are retained based on average up-time. New log files are only started when the system is restarted. The current settings will provide a retention period exceeding 120 days.

Network Traffic Monitoring - EPA's network traffic monitoring had limited capacity and did not include monitoring of contractor connections. NIST guidance states that organizations should employ tools and techniques to monitor events on information systems, detect attacks, and identify unauthorized use of the system. This includes monitoring inbound and outbound communications for unusual or unauthorized activities or conditions, and employing traffic profile analysis to detect deviations from the volume or types of traffic expected within the organization. However, EPA's network monitoring tool (Scrutinizer Netflow Traffic Analysis) used to monitor inbound and outbound traffic was set to retain only 14 days of traffic data for main internal connections and did not collect network traffic data for contractor connections. As a result, malicious users or intruders could attempt attacks against EPA networks and computers with reduced likelihood of detection.

GAO Recommendations:
60. Capture a greater amount of network traffic data sufficient for network traffic analysis in detecting unusual or unauthorized activities or conditions and deviations from expected volumes or types of traffic.
61. Capture network traffic data for contractor connections.

EPA Response:
The EPA concurs with the recommendations. The EPA is currently reviewing options to provide a tool that will maintain a minimum of 1 year of traffic analysis data. The EPA has employed the use of Scrutinizer on the contractor connections.

PHYSICAL SECURITY

Access Authorizations - EPA did not always appropriately restrict or authorize access to the National Computer Center at Research Triangle Park. NIST guidance recommends that organizations develop and keep current a list of personnel who have authorized access to the facility where information systems

reside (except for those areas within the facility officially designated as publicly accessible). Five EPA employees and contractor staff, who were not on the authorized access list, were able to use their badges to gain access to the computer room and its sensitive resources. As a result, the agency has less assurance that physical access controls are being implemented as intended.

GAO Recommendation:
62. Update authorized access lists to include currently authorized personnel or remove access for those no longer requiring it.

EPA Response:
The EPA concurs with the recommendation.

- NCC compared and analyzed data from three sources for the time period in question, namely the week of August 8-12, 2011. Data sources were: (1) the NCC authorized access list archive covering this time period; (2) the OARM-RTP master personnel access list archive covering this time period; and (3) the physical card reader access logs for all NCC raised floor card readers covering this time period. NCC's review and analysis offers these observations:
- From the NCC raised floor card reader logs, 18 people gained access to the computer room that were not on the NCC authorized access list archive.
- Of these 18 people, 13 were authorized by the OARM-RTP master personnel access list archive.
- The five remaining people were Federal NCC employees, who gained access as a result of a discrepancy with raised floor card readers that were inadvertently assigned to another NCC access right. According to OARM-RTP, this discrepancy probably occurred during the migration of the old legacy reader access system to its current replacement facility commander system. This discrepancy was corrected upon its discovery in mid-August 2011 by OARM-RTP.

Visitor Control Log - EPA did not always effectively log visitors at its National Computer Center, Research Triangle Park location. NIST recommends that organizations control all physical access points to their computer facilities and access to information systems independent of the physical access controls for the facility. It also recommends that organizations maintain and review visitor access records to facilities housing information systems and that these records include the name, signature, and organization of the visitor, form(s) of identification, date of access, time of entry and departure, and purpose of the visit, among other things. However, visitors' access control records at the National Computer Center, Research Triangle Park, North Carolina, were not always complete. Visitor logs for server rooms, one of which contained a badging server, and a telecom room did not include information such as visitor's identification, purpose of visit, and time of departure from the rooms. As a result, the agency has reduced assurance that controls are in place to ensure that visitors have an appropriate need to access EPA's computing facilities.

GAO Recommendation:
63. Ensure visitor access log information is complete and includes the visitor's identification, purpose of visit, and exit time.

EPA Response:
The EPA concurs with the recommendation. The server rooms addressed in this report as well as the remaining server rooms identified in the Agency's FDCCI list for the EPA-RTP campus have been decommissioned. Servers have either been moved to the NCC Data Center or the RTF Silo Room.

This list of decommissioned server rooms includes: C160, C131, C240, E460, E460A, E455, E485, and N147. The decommissioning process began in July 2011 with Server Room C160 and completed with the decommissioning of Server Rooms C131 and N147 in May 2012.

CONFIGURATION MANAGEMENT

Virtual Local Area Network Configuration - EPA did not securely configure virtual local area networks on its Cisco network switches. NSA guidance states that Cisco, as a broadcast domain designed to not receive packets sent by a different virtual local area network should be logically separated along functional lines. This includes not using Cisco's default 1 for either out-of-band management or in-band management because it may span an entire network (across many others) and provide attackers easier access and extended reach for their attacks. Additionally, native virtual local area networks should not be assigned to an active virtual local area network. However, EPA did not always adequately configure its virtual local area networks. For example:

- The default virtual local area network 1 was used on many EPA network switches for management of traffic (e.g., devices related to icc, rio, and pyd locations).
- Virtual local area network access was not restricted from spanning EPA's entire enterprise network.
- EPA assigned native virtual local area networks to active virtual local area networks, including in areas where switchports were connected to IP phones that were connected to computers and where some were located in untrusted areas. By assigning native virtual local area networks to active virtual local area networks, the identity enforcement functionality that virtual local area network tagging creates could be undermined.

As a result of these weaknesses, EPA's network was susceptible to known vulnerabilities that could allow an individual with access to a virtual local area network to obtain unauthorized access to another virtual local area network.

GAO Recommendations:
64. Prohibit the use of a virtual local area network 1 for management of traffic.
65. Restrict virtual local area networks from unnecessarily spanning EPA's enterprise network.
66. Do not assign a native virtual local area network to an active virtual local area network.

EPA Response:
The EPA concurs with the recommendations.

- Recommendation 64 - The Potomac Yard and 1310 L Street sites were completed at the end of 2012, as a component of the HQ Core Switch Upgrade - Phase I. Federal Triangle will be fixed by the end of the 3rd quarter in FY '13 once the distribution switches have been upgraded. The EPA will not use vlan 1. There will be separate native vlan with no SVI. Management will be handled by another network. A plan of action and milestones will be created to remove VLAN 1 with a tentative completion date of the beginning of the 4th quarter of FY '13.
- Recommendation 65 – The EPA is following best industry practices by creating VLANs only when operationally necessary, and defining VLANs as a subnet to be able to manage and limit broadcasting across multiple VLANs. A plan of action and milestones will be created to prune Federal Triangle after the installation of the new distribution switches with a tentative completion date of April 30, 2013.
- Recommendation 66 – The Potomac Yard and 1310 L Street sites were completed at the end of 2012, as a component of the HQ Core Switch Upgrade - Phase I. Federal Triangle will be fixed

by the end of the 3rd quarter in FY '13 once the distribution switches have been upgraded. We will not use vlan 1. There will be separate native vlan with no SVI. Management will be handled by another network. A plan of action and milestones will be created to remove VLAN 1 with a tentative completion date of the beginning of the 4th quarter of FY '13.

Network Device Services - EPA enabled the Internetwork Packet Exchange routing protocol on several network devices. The protocol is a legacy Novell routed protocol that was used as an alternative to IP on Novell platforms. NSA guidance states that routers should support only traffic and protocols needed by the network and that unnecessary services should be disabled in the router configuration. However, the Internetwork Packet Exchange Routing Protocol was unnecessarily enabled on 10 network devices where most firewalls and intrusion detection systems could not inspect Internetwork Packet Exchange Routing Protocol traffic. Moreover, security and operational updates to the protocol were no longer provided. As a result, EPA may be vulnerable to Internetwork Packet Exchange Routing Protocol security weaknesses.

GAO Recommendation:
67. Disable Internetwork Packet Exchange Routing Protocol routing on all network devices.

EPA Response:
The EPA concurs with the recommendation and has corrected the weakness. The office (OCSPP) using IPX Protocol has been converted to IP. This occurred in October 2012.

E-Mail Host Configuration - EPA did not adequately filter e-mail attachments and spoofed messages to prevent activity that could be malicious. NIST guidance states that organizations should configure e-mail systems to filter content and take precautionary measures to prevent activity that is likely to be malicious. NIST emphasizes that organizations should take steps to prevent e-mail address spoofing, including ensuring that external users cannot send e-mails to internal users that have one of the organization's e-mail addresses as the spoofed sender.[29] However, EPA did not adequately filter e-mail attachments and prevent spoofing to prevent activity that was likely to be malicious. For example, the EPA Internet e-mail gateways did not adequately implement spoofed e-mail protection, where current practice is to apply anti-spam filter checking with specific rules in place to increase chances for quarantine as spam, but not enough to block the e-mail message for that reason alone. Moreover, the blacklist approach for e-mail attachments used by the e-mail system had limitations because there are many known and unknown attachments that could be potentially dangerous that were not blacklisted (e.g., .bin, .mht, .command, and some but not all .dll). In addition, there were no e-mail gateway products that could detect malware or inspect links to malicious content. As a result, increased risks exist that an attacker using an allowable e-mail attachment file type could successfully distribute malware such as viruses, Trojans, key loggers, spyware, adware, and rootkits; that users could be lured into revealing passwords or other confidential information; and that denial-of-service attacks could be successful.

GAO Recommendations:
68. Filter all e-mail attachments by default and only allow specified file types as attachments or ensure that all dangerous attachments are blocked.
69. Fully prevent spoofed e-mails from being sent by taking steps beyond the use of spam filtering.

[29] E-mail spoofing occurs when a user receives e-mail that appears to have originated from one source when it actually was sent from another source. E-mail spoofing is often an attempt to trick the user into making

EPA Response:
The EPA concurs with the recommendations and has created a plan of action and milestones for remediation. This will be corrected in the new Email and Collaboration to the Cloud project.

Patch Management - EPA did not consistently implement patches for several systems reviewed. NIST guidance recommends that organizations promptly test and install newly released security patches, service packs, and hot fixes. However, EPA did not consistently apply patches to critical systems or patch applications in a timely manner. Specifically, several critical systems had not been patched or were out of date, some of which had known vulnerabilities. The following are examples:

- 53 Cisco network devices were missing Internetwork Operating System patches.
- Five Red Hat Linux servers using versions ranging from 4 thru 5.6 were not applying the latest operating system version 6.2 applicable to the eGGRT applications and infrastructure servers.
- Three Windows 2008 servers related to CDX were missing two critical operating system patches and one important operating system patch from June and May 2011. The critical patches mitigate a vulnerability, permitting remote code execution and a vulnerability that could allow elevation of privileges.
- The domain controller for the Office of Pollution Prevention Technology division's CBI network was missing patches from October 2010 through February 2011.
- Nine Oracle databases missing critical patch updates had not been patched since April 2010 for six databases and April 2011 for three databases supporting these software applications: CBITS, the CDX applications, and OAS/OCS.
- The latest build/hot fix was not installed for EPA's VCenter VMware MS SQL 2008 server database system that is used in support of centrally managing ESXi servers.
- Seven Unix servers were running unpatched versions of Java in support of the CAMDBS, eGGRT, and SEMS applications.
- 5 Unix-based servers' Apache web applications were missing security patches supporting the SEMS, CAMDBS, and eGGRT applications.
- Two Unix-based servers with OpenSSL were missing security patches related to SEMS and OAS applications.
- Two Windows CDX servers, the DMZ Active Directory domain controller and the SEMS production application web server, were missing the cumulative security patch for Internet Explorer 8 that was released on August 9, 2011.
- One Unix server had an unpatched version of Samba.

As a result of these conditions, increased risk exists that unpatched vulnerabilities could be exploited.

GAO Recommendation:
70. Apply the latest patches to the systems identified.

EPA Response:
In response to the network related recommendations, the EPA will work with GAO to identify issues with the 53 Cisco devices. Detailed information such as required patch level and specific vulnerability associated with current IOS levels are needed in order to address this finding.

In response to the hosting related recommendations, all OEI/OTOP/NCC servers that were missing patches have been fully updated\patched.

- OCSPP – CISCO Switches; the bear term action plan is to update the switches. The long term solution will have OEI/OTOP/EDSD to manage the OPPT switches.
- Oracle 11g and SQL; servers will be upgraded with version control patches. Patch management will be performed and maintained regularly as part of the system maintenance procedures. Oracle databases have been patched to the October 2012 PSU level. The VMWare SQL Servers are running version 2008 R2 with Service Pack 1 applied.
- Domain Controller; OCSPP is working with OEI/OTOP/NCC to implement a process to update the system patches and maintain them under the system maintenance procedures.
- Unix/Samba: Further clarification has been requested from GAO to determine if the Unix server missing the updated SAMBA patch is part of the OCSPP hardware inventory.
- Internet Explorer; OCSPP is working with NCC to implement a process to update the system patches and maintain them under the system maintenance procedures.
- OIC and OAR systems have been remediated.

Cisco Discovery Protocol - EPA enabled the Cisco Discovery Protocol on network devices (accessible to users and the general public). The Cisco Discovery Protocol is a proprietary protocol that allows a device to advertise its existence to other devices and receive information about other devices on the same LAN or on the remote site of a WAN. Cisco recommends disabling the protocol since it can cause information about the network to be leaked to potential attackers. However, EPA had not disabled the Cisco Discovery Protocol on network switches. As a result, devices on EPA's network were susceptible to attackers being able to gather information about EPA's network.

GAO Recommendation:
71. Disable the Cisco Discovery Protocol on network devices when there is no operational need for the protocol.

EPA Response:
The EPA concurs with the recommendation and has corrected the weakness. The EPA reconfigured devices to only operate CDP on links between managed devices and trunk ports on May 23, 2012. In addition, the EPA has validated that all switches have been configured to the EDSD SCD which states that CDP on links between managed devices and trunk ports; this was completed October 19, 2012.

Simple Network Management Protocol - EPA did not always securely implement the Simple Network Management Protocol.[30] NIST states that organizations should configure the security settings to the most restrictive mode consistent with operational requirements. In addition, NSA states that the use of Simple Network Management Protocol versions 1 and 2 are insecure and suggests that organizations use version 3. However, EPA used versions 1 and 2 on its network devices that transmit credentials and other sensitive data in clear text. Furthermore, this protocol was enabled in read/write mode on most devices, which could allow an unauthorized user to modify and control the configuration of these devices, thereby facilitating the introduction of many other security weaknesses, including access to unencrypted and weakly encrypted passwords. On many devices, compensatory controls such as access control lists were not used to control read/write privileges. As a result of these weaknesses, increased risk exists that malicious individuals could gain access to, change the configuration of, or disrupt networks.

[30] The Simple Network Management Protocol is a standard protocol for remote management and monitoring of network devices that uses unencrypted community strings as passwords for authentication.

GAO Recommendation:
72. For all network devices using Simple Network Management Protocol, use the secure Simple Network Management Protocol version 3 or, if using Simple Network Management Protocol versions 1 and 2, configure in read mode.

EPA Response:
The EPA partially concurs with the recommendation. All current OARM-RTP devices are using SNMP v2 in the Read Only mode with the following two exceptions: Ciscoworks and Kiwi, which reside on the same device and Opmanager, located on a separate server. These network management tools allow us to perform automated functions; without them we cannot proactively manage the network, with the result being unscheduled down time. These network management tools are critical to the performance of the EPA-RTP local area network and cannot be arbitrarily shut down.

To address the protocol issue, the EPA plans to upgrade the aforementioned network management tools to utilize SNMP v3, as part of the EPA-RTP campus Telecom Switch Upgrade Project. This project will begin in the first quarter of fiscal year 2013. SNMP v3 will be implemented with guidance provided by OEI since SNMP v3 has not yet been adopted as an Agency standard.

Network Devices Configuration - EPA did not adequately configure network devices to prevent security vulnerabilities. NIST states that, based on organizations' operational needs, information systems should be set to the most restrictive mode. However, network devices were not appropriately configured, as the following examples illustrate:

- The Web Cache Communication Protocol[31] enabled on EPA routers as a load-balancing, content-routing protocol to redirect traffic flows in real-time had the MD5 authentication feature disabled and had mis-configured re-direct access control lists. Additionally, group access control lists were not used in restricting access to the Web Cache Communication Protocol.
- DLSw tunnels, which are created to tunnel unroutable, non-IP protocols through an IP network, were active on EPA routers. For example, DLSw tunnels are used to tunnel IBM mainframe systems network architecture through an IP network.

As a result, these routers are vulnerable to a man-in-the-middle attack by an attacker who is redirecting all traffic to their site by using a network sniffer and also to attackers creating a covert communication path into EPA's network.

GAO Recommendations:
73. Enable MD5 authentication for the Web Cache Communication Protocol.
74. Properly configure group access control lists to restrict access to the Web Cache Communication Protocol.
75. Disable all DLSw tunnels that are no longer needed.

EPA Response:
The EPA concurs with the recommendations and has corrected the weaknesses as follows.

- Recommendations 73 & 74 - MD5 has been implemented and ACLs updated.

[31] The Web Cache Communication Protocol is a Cisco-developed content-routing protocol that provides a mechanism to redirect traffic flows in real time. It has built-in load balancing, scaling, fault tolerance, and service-assurance (failsafe) mechanisms.

- Recommendation 75 - There is (1) DLSw tunnel remaining and that is part of a legacy system belonging to the VA.

Voice over Internet Protocol Configuration - The EPA's Voice over Internet Protocol (VoIP) system was not securely configured. NIST states that organizations should configure security settings to the most restrictive mode consistent with operational requirements. However, VoIP systems were not appropriately configured, as the following examples illustrate:

- Telnet was used remotely by administrators to access the Avaya VoIP administration server where all credentials and data are sent in clear text.
- Two servers (Redsky E911 and BCMS) were assigned "superuser" privileges when automatically accessing the VoIP administration server. This allows an attacker who compromises either server to have root-level access to the Avaya VoIP system.
- The Redsky E911 server, which handles 911 functional requirements for the VoIP system, had outbound Internet access when there was no operational need for this level of access. The administrator demonstrated access to various Internet websites.
- Unauthorized remote access software was running on the Redsky E911 server and had not been removed.
- The Windows firewall was not enabled, which allowed any inbound connection to access the Redsky E911 server.

As a result, risk is heightened that EPA's VoIP could be compromised; giving a perpetrator unauthorized access and control of VoIP system resources.

GAO Recommendations:
76. Discontinue use of Telnet for remote administration.
77. Assign lower privileges to systems automatically accessing the VoIP site administration server.
78. Restrict outbound access to the E911 server to only operational requirements.
79. Uninstall the unauthorized remote access software.
80. Enable Windows firewall on the Windows-based E911 server.

EPA Response:
The EPA concurs with the recommendations.

- Recommendation 76 – The telnet is not in use for outbound alarm usage between the ION Defender and the Avaya voice system. It was turned on for the inbound portion of the session between the ION Defender and the Avaya voice system. Telnet will not be required if Secure Access Link (SAL) is approved for access to the voice system. A POA&M will be created to address the transition to SAL and eventually turning off Telnet.
- Recommendation 77 - The HQ Avaya voice system was upgraded from January thru May 2012. No systems automatically access the VOIP site administration server in the present configuration. The RedSky e911 server has been removed. BCMS does not have automatic access to the VOIP administration server; however access to the VOIP administration server from BCMS is directly recognized as BCMS in lieu of a specific userid and has no "superuser" privileges. Access rights of BCMS are the same as other userids who access the VOIP server for VOIP administration.
- Recommendation 78 - The HQ Avaya voice system was upgraded from January thru May 2012. The RedSky e911 system has been removed and is not being used in the present configuration.

- Recommendation 79 - The HQ Avaya voice system was upgraded from January thru May 2012. No remote access software is installed on the present configuration of the Avaya Communication Manager, Avaya Modular Messaging. The RedSky e911 has been removed and is not being used in the present configuration.
- Recommendation 80 - The HQ Avaya voice system was upgraded from January thru May 2012. The RedSky e911 system has been removed and is not being used in the present configuration.

VoIP Access Switches - EPA did not adequately secure its network access switches that control its VoIP network. NIST guidance recommends encrypting voice calls to prevent unauthorized users from eavesdropping on voice sessions and other traffic sent in clear text such as used for backing up network configurations. Cisco best practices also recommend the use of Dynamic Address Resolution Protocol Inspection and IP Source Guard when implementing Dynamic Host Configuration Protocol snooping[32] to prevent Address Resolution Protocol poisoning and IP spoofing.[33] However, EPA did not encrypt its voice calls or implement Dynamic Address Resolution Protocol Inspection and IP source guard on all access switches used with Dynamic Host Configuration Protocol snooping to assure the security of the server allocating VoIP addresses to valid clients. Consequently, EPA is at risk that unauthorized users could eavesdrop on voice sessions. Moreover, without the control mechanisms implemented, an attacker could manipulate Address Resolution Protocol tables and IP addresses, and redirect local area network traffic to where worms and other malware use IP and Address Resolution Protocol spoofing techniques to disguise their origins.

GAO Recommendations:
81. Implement encryption on voice calls.
82. Implement Dynamic Address Resolution Protocol Inspection and IP Source Guard on all access switches with Dynamic Host Configuration Protocol snooping.

EPA Response:
- Recommendation 81 - The EPA concurs with the recommendation and a plan of action and milestones has been created to enable encryption.
- Recommendation 82 - The EPA could neither concur or nonconcur with this recommendation. The EPA requests clarification from GAO on what devices, where they are located, and what the security issue is with the devices to warrant implementation of a Dynamic Address Resolution Protocol.

MS SQL Database Configuration - EPA did not securely configure the MS SQL database system for its VCenter VMware MS SQL 2008 server database system. NIST states that organizations should configure security settings to the most restrictive mode consistent with operational requirements. However, EPA's VCenter MS SQL database, which is used in support of centrally managing ESXi servers, was not appropriately configured, as the following examples illustrate:

---

[32] In computer networking, Dynamic Host Configuration Protocol snooping is a series of techniques applied to ensure the security of an existing Dynamic Host Configuration Protocol infrastructure. When Dynamic Host Configuration Protocol servers are allocating IP addresses to the clients on the LAN, Dynamic Host Configuration Protocol snooping can be configured on LAN switches to harden the security on the LAN to allow only clients with specific IP/Media Access Control addresses to have access to the network.

[33] Address Resolution Protocol poisoning allows an attacker to alter routing on a network (i.e., man-in-the-middle attack), and IP spoofing refers to the creation of IP packets with a forged source IP address.

- The xp_cmdshell function as a server configuration option was enabled. It allows users with access to execute any command on the operating system, since it runs with the privileges of the account that the SQL server is running (normally the powerful SYSTEM account).
- The SQL server agent and server service[34] were running as Local System, which is a powerful account that has full access rights to the computer and is a member of the Windows administrators group. This would enable an attacker to take complete control of the database server and the host operating systems by exploiting a vulnerability found in the agent or server service.
- The MS SQL Simple Network Management Protocol registry key was enabled, which allowed community strings to be read from the registry and may represent a broader threat to the network than just the server.

As a result, risk is heightened that EPA VCenter database, server, and potentially other network resources could be compromised.

GAO Recommendations:
83. Remove or restrict access to the xp_cmdshell.
84. Change the SQLO server aent and servr service to operate as a low privileged domain or local account.
85. Disable the SNMP registry key or, if it is necessary to keep it enabled, ensure that appropriate permissions are applied.

EPA Response:
The EPA concurs with the recommendations and has corrected the weaknesses. All agents have been updated to comply with this recommendation. This action was taken as part of the security review. The EPA removed access to the xp_cmdshell, changed the SQL server agent and server service to operate as a low privileged domain or local account, and disabled the SNMP registry key.

Outdated Software - EPA used outdated versions of software and products that were no longer supported by the vendor. NIST guidance states that organizations should promptly test and install the newly released security patches, services, and hot fixes as soon as they become available. However, EPA was using out-of-date or unsupported software and products, as illustrated in the following examples:

- Three Cisco network routers were using platforms that had reached the end of life support:
- A National Computer Center router (ncc-svr-s1) using the Cisco CATOS operating system, which provides connectivity to many sensitive devices such as two terminal console servers used for out-of-band network management, a jump server for logon to network devices, TACACS+ server, and a network syslog server (ncc-svr-s1).
- A National Computer Center, Research Triangle Park, Systems Network Architecture[35] router using the Cisco 2621 platform for network tunneling capabilities in transmitting mainframe

[34] SQL Server Agent is a Microsoft Windows service that executes scheduled administrative tasks, which are called jobs. The SQL Server service runs the database engine. There is one SQL Server service for each instance of SQL Server running on a computer.
[35] Systems Network Architecture, IBM's proprietary networking architecture, was first introduced in 1974.

Systems Network Architecture traffic across EPA's IP network (Rapid Transport Protocol-Systems Network Architecture using a Cisco 2621 platform).

- A National Computer Center router (EXT-C1) using the Cisco IOS RSP software that was providing connectivity between EPA's National Computer Center and the National Oceanic and Atmospheric Administration.
- The National Computer Center was using a Network Simple Network Management Protocol server with HP-Openview Network Node Manager version 6.2, which had reached its end of life on December 31, 2007.
- The database supporting EPA's CBITS application was using Oracle 8.1.7.4.1, which is an unsupported version of Oracle as of December 31, 2004.
- Eight servers providing application support were using RedHat Linux version 3 operating systems, which are at their end of life. EPA had not purchased "extended life cycle" support.

Using outdated or unsupported products increases the risk that an attacker may exploit vulnerabilities associated with these products.

GAO Recommendation:
86. Upgrade to vendor-supported versions of these software products.

EPA Response:
The EPA concurs with the network related recommendation and has corrected the weakness and is working to replace HP Open View with EM7, the network syslog server (ncc-svr-sl) was decommissioned, and all Red Hat Version 3 systems have been removed and replaced with Red Hat Version 6 systems. The EPA purchased a maintenance agreement and license for the Oracle application from the vendor. CIS and the Oracle application will be upgraded as notified by the vendor.

CBITS is being retired in March 2013 and the new system with rely on Oracle 11g.

Switches - EPA had not always implemented security measures to protect switches from vulnerabilities when using the Spanning Tree Protocol.[36] Cisco recommends, as part of this protocol, that organizations enable the Spanning Tree Bridge Protocol Data Unit[37] Guard and Root Guard on switches. Bridge Protocol Data Unit Guard prevents a particular physical network port interface from being used (accidentally or maliciously) as a root bridge, which could crash an entire network or network segment. Root Guard is used to ensure certain ports on switches upstream from the access switches never become the root bridge. Root Guard also allows the device to participate in Spanning Tree Protocol as long as the device does not try to become the root bridge. However, EPA did not always adequately protect switches because Bridge Protocol Data Unit Guard was not enabled on switchports that were connected to user workstations and servers. Additionally, Root Guard was not enabled on EPA switches that restrict upstream switchports from trying to become the root bridge. As a result, a malicious user could adversely affect network operations and capture sensitive data by falsely becoming the root bridge.

[36] The Spanning Tree protocol is a link layer network protocol that ensures a loop-free topology for any bridged local area network (i.e., used to cut loops that redundant links create in bridge networks).
[37] Bridge Protocol Data Unit messages are used in determining what switch will be the root bridge/port where all traffic flows through. Because the protocol does not have a way to verify the authenticity of Bridge Protocol Data Unit messages, an attacker can spoof it and compromise network traffic without using control measures.

GAO Recommendation:
87. Implement Bridge Protocol Data Unit Guard and Root Guard to protect EPA's networked switched environment.

EPA Response:
The EPA concurs with the recommendation.

- On June 10, 2012 under CRQ#6181, the EPA completed the following tasks: (1) Root Guard was applied to trunked interfaces south of the STP Root devices towards STP leaf devices; and (2) Loop Guard was applied to trunked interfaces north of the STP Leaf devices towards STP root devices
- At the end of 2012, the Potomac Yard and 1310 L Street were completed as a component of the HQ Core Switch Upgrade - Phase I.
- Federal Triangle will be fixed by the end of the 3rd quarter in 2013 once the distributions switches have been upgraded.

Exceed Configuration - EPA did not adequately configure security settings on a jump server used to logon to network devices in its Central Data Exchange environment. NIST states that organizations should configure security settings to the most restrictive mode consistent with operational requirements. EPA used the Exceed application to connect its Microsoft Windows jump server to the X-Windows[38] environment. However, the server was not configured to its most restrictive mode. Specifically, the Exceed application was not configured to restrict access, which would allow an attacker to capture all screen inputs from the server. As a result, increased risk exists that sensitive information could be compromised.

GAO Recommendation:
88. Configure the Exceed software on the jump server to restrict access.

EPA Response:
The EPA concurs with the recommendation. Hosting jumpboxes have been patched and reconfigured.

Hypertext Transfer Protocol Configuration - EPA had the Hypertext Transfer Protocol server feature enabled on a router used to establish site-to-site VPN connections for its contractors into the EPA production network. NSA guidance states that network devices should be appropriately configured to protect organization information assets, including disabling the Hypertext Transfer Protocol server, as it is susceptible to several Hypertext Transfer Protocol privilege escalation vulnerabilities. However, EPA had the Hypertext Transfer Protocol server feature enabled on its VPN router. As a result, the device is susceptible to compromise in that a perpetrator could gain full control over these devices by exploiting Hypertext Transfer Protocol privilege escalation vulnerabilities.

GAO Recommendation:
89. Disable use of the Hypertext Transfer Protocol server feature on the router used to establish contractors' site-to-site VPN connections into the EPA production network.

EPA Response:
The EPA concurs with the recommendation and has corrected the weakness. The EPA made the following changes to address the finding on NCC-NSOC-VPN: (1) enabled password encryption; (2)

[38] X-Windows is a standard for a platform-independent, network-based graphical user environment.

enabled encryption of VPN pre-shared keys; (3) changed the default password; (4) added account of last resort; (5) corrected Access Control Lists; (6) disabled Telnet and HTTP services; (7) added welcome banner; added AAA authentication; and (8) upgraded IOS to FIPS 140-2 approved encryption standards.

MEDIA DESTRUCTION AND DISPOSAL

Testing Equipment - EPA did not provide evidence that it had tested equipment to sanitize and dispose of media at Washington, D.C., and Research Triangle Park, North Carolina, locations. NIST states that testing is required for equipment used in sanitization of media. However, EPA did not provide evidence of testing hard drive wiping equipment in the CBITS environment at EPA headquarters and did not provide evidence of testing degaussers in the WAN and National Hosting Systems environments at the National Computer Center, Research Triangle Park. As a result, EPA has less assurance that equipment used to remove sensitive information is operating as intended.

GAO Recommendations:
90. Document testing of the hard drive wiper at EPA in the CBITS environment.
91. Document testing of the degaussers at the National Computer Center in the WAN and National Hosting Systems environments.

EPA Respone:
The EPA concurs with the recommendations. The media sanitization procedures are being revised to include testing as part of the security wipe process. The EPA has added a Degausser section into the Data Center Standards and Procedures Manual which specifies and documents Degausser testing.

Sanitization Records - EPA did not document records of media sanitization at the Washington, D.C., and Research Triangle Park, North Carolina, locations. NIST recommends that organizations maintain records of what media were sanitized, when, how they were sanitized, and the final disposition. However, EPA did not document such records of media sanitization at the CBITS environment at the headquarters location and in the WAN and National Hosting System environments at the National Computer Center, Research Triangle Park. Until EPA documents records of media disposal, the agency may have less assurance that sensitive information is sanitized before media has been disposed.

GAO Recommendations:
92. Document media sanitization at EPA in the CBITS environment.
93. Document media sanitization at EPA in the WAN and National Hosting System environments.

EPA Response:
The EPA concurs with the recommendations. The media sanitization procedures are being revised to include records retention as part of the security wipe process. The EPA has corrected the weakness. The EPA has added a Degausser section into the Data Center Standards and Procedures Manual which also covers media sanitization.

Hard Drive Labels - EPA did not properly label hard drives containing sensitive information and document records of media sanitization at the Washington, D.C., location in its CBITS environment. NIST states the organization should mark removable information system media and information system output as well as indicate the distribution limitations and applicable security markings of the information. However, hard drives that may have contained sensitive or confidential business information, which were to be wiped of such information, were not labeled to distinguish them from

drives that had been wiped of sensitive information. In addition, there were numerous hard drives that may have contained sensitive information stacked beside those where the information had been wiped, but there were no distinguishing markings or labels on the drives. As a result, EPA has increased risk that sensitive information may not be properly protected.

GAO Recommendation:
94. Label hard drives containing sensitive information until the information has been removed.

EPA Response:
The EPA concurs with this recommendation. The media sanitization procedures are being revised to include the proper labeling of CBI hard drives used to process and store sensitive information as part of the security wipe process.

VAL13-000-3370

UNITED STATES ENVIRONMENTAL PROTECTION AGENCY
WASHINGTON, D.C. 20460

MAR 28 2013

OFFICE OF THE
CHIEF FINANCIAL OFFICER

The Honorable Harold Rogers
Chairman
Committee on Appropriations
U.S. House of Representatives
Washington, D.C. 20515

Dear Mr. Chairman:

I am transmitting the U.S. Environmental Protection Agency's response to the December 2012 Government Accountability Office report entitled, *Environmental Protection: EPA Should Develop a Strategic Plan for Its New Compliance Initiative* (GAO-13-115). The EPA prepared this response pursuant to 31 U.S.C. 720.

In its review, the GAO examined (1) actions the EPA has undertaken in Next Generation Compliance to increase transparency and accountability and (2) the extent to which the EPA is developing a strategic plan to integrate Next Generation Compliance into its enforcement and compliance program.

GAO Recommendation

To better integrate Next Generation Compliance into its overall enforcement and compliance program and ensure that the initiative will achieve the goals the EPA envisions for it, we recommend that the Administrator of EPA direct the Assistant Administrator of OECA to take the following two actions:

- Develop a schedule for completing, in a timely manner, a strategic plan for Next Generation Compliance; and
- Ensure that this strategic plan incorporates selected leading practices in federal strategic planning, as appropriate, and describes how Next Generation Compliance is to be integrated into the enforcement and compliance program.

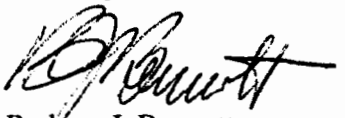
EPA Response

The EPA agrees with the GAO's recommendation that the agency should prepare a strategic plan for the Next Generation Compliance initiative in FY 2013, and we believe the work done so far and underway on Next Generation Compliance will provide a foundation for a thoughtful and well-informed plan. The EPA expects to develop a schedule for completing a strategic plan by March 30, 2013. However, under the continuing resolution, the EPA cannot start any new initiatives. The EPA further agrees that the

strategic plan should incorporate, where appropriate, leading practices in federal strategic planning and describe how Next Generation Compliance will be incorporated into the compliance and enforcement program.

The EPA appreciates the GAO's review of these issues and the opportunity to review and respond to the GAO's report. If you have any questions, please contact me or your staff may call Christina Moody, in the EPA's Office of Congressional and Intergovernmental Relations, at (202) 564-0260.

Sincerely,



Barbara J. Bennett
Chief financial Officer

AL 14-000-8901

UNITED STATES ENVIRONMENTAL PROTECTION AGENCY
WASHINGTON, D.C. 20460

MAY - 9 2014

OFFICE OF THE
CHIEF FINANCIAL OFFICER

The Honorable Harold Rogers
Chairman
Committee on Appropriations
U.S. House of Representatives
Washington, D.C. 20515

Dear Mr. Chairman:

I am transmitting the U.S. Environmental Protection Agency's response to the January 2014 Government Accountability Office report entitled, *EPA has Improved its Unregulated Contaminant Monitoring Program, but Additional Action is Needed* (GAO-14-103). The EPA prepared this response pursuant to 31 U.S.C. 720.

The agency appreciates the GAO's acknowledgment that the EPA has effectively addressed recommendations from its prior report on this subject, *Safe Drinking Water: EPA Should Improve Implementation of Requirements on Whether to Regulate Additional Contaminants* (GAO-11-254). The EPA generally agrees with the GAO's "Recommendations for Executive Action" and we plan to address those recommendations as described below.

GAO Recommendation

The Administrator of the Environmental Protection Agency should direct the Assistant Administrator of the Office of Water to help ensure that the UCMR [Unregulated Contaminant Monitoring Rule] data accurately reflect contaminant occurrence, vary the monitoring frequency for public water systems when the standard UCMR monitoring frequency is not expected to accurately detect the presence of contaminants, such as sporadically occurring viruses or pesticides that fluctuate seasonally.

EPA Response

Beginning with the development of the rule for the next UCMR cycle ("UCMR 4"), the EPA will give greater consideration to the potential for particular contaminants to occur sporadically and/or seasonally. To the extent practical, taking into account factors such as cost and implementation considerations, the agency will seek to adjust the monitoring frequency for contaminants that are anticipated to have significant sporadic and/or seasonal occurrence.

GAO Recommendation

The Administrator of the Environmental Protection Agency should direct the Assistant Administrator of the Office of Water to help address potential limitations with the UCMR data, when considering if adequate data had been collected under a prior UCMR during the contaminant selection process, take

into account whether: (1) the sampling methodology EPA used in a prior UCMR for a particular contaminant provided sufficient occurrence data to make a regulatory determination, (2) the contaminant's health information is in flux or has been updated and now indicates that adverse health effects occur at a lower level than that at which UCMR data were originally collected, or (3) the data collected in an earlier cycle have become outdated and no longer present an accurate picture of contaminant occurrence, for example, because industrial or agricultural chemical use has changed.

EPA Response

Beginning with the development of the rule for UCMR 4, the EPA will give greater consideration to whether additional occurrence data gathering is warranted for contaminants monitored during prior UCMR cycles. The agency will specifically consider (1) the sampling methodology used in the prior cycle; (2) changes in health information (e.g., establishment of a lower health reference level) that may warrant additional monitoring at a lower level; and (3) the degree to which the available data are expected to be representative of current contaminant occurrence. These factors will be considered in the agency's establishment of relative priorities for UCMR contaminant selection. As to the use of the UCMR data from prior cycles to support the agency's regulatory determinations, the EPA will continue to judge the appropriateness of the data on a case-by-case basis. As acknowledged in the report, the agency uses the "best available" data to support its decisions.

GAO Recommendation

The Administrator of the Environmental Protection Agency should direct the Assistant Administrator of the Office of Water to optimize the ability of the UCMR program to support regulatory determinations, convene an internal working group of officials responsible for the UCMR, regulatory determinations, and CCL [Contaminant Candidate List] to fully examine opportunities to improve the timeliness of the UCMR program. Among other things, the working group should consider: (1) whether a shorter process for selecting contaminants would yield a high-quality list, or whether the existing process can be started sooner, and (2) whether monitoring for contaminants over a shorter period, instead of the current 3-year period, is feasible, given data quality, logistical needs, and the burden on public water systems.

EPA Response

The EPA will convene the recommended workgroup and will consider, among the potential improvements, the practicality of a shorter process for contaminant selection and a shorter period for contaminant monitoring. Workgroup recommendations will be incorporated into our approach to the extent practical.

The EPA expresses its appreciation for the thoughtful work and professionalism of the GAO staff members throughout this review. If you have any further questions, please contact me or your staff may contact Christina Moody in the EPA's Office of Congressional and Intergovernmental Relations, by phone at (202) 564-0260, or by email at moody.christina@epa.gov.

Sincerely,

Maryann Froehlich

Maryann Froehlich
Acting Chief Financial Officer

UNITED STATES ENVIRONMENTAL PROTECTION AGENCY
WASHINGTON, D.C. 20460

MAY - 9 2014

OFFICE OF THE
CHIEF FINANCIAL OFFICER

The Honorable Thomas R. Carper
Chairman
Committee on Homeland Security and Governmental Affairs
United States Senate
Washington, D.C. 20510

Dear Mr. Chairman:

I am transmitting the U.S. Environmental Protection Agency's response to the January 2014 Government Accountability Office report entitled, *EPA has Improved its Unregulated Contaminant Monitoring Program, but Additional Action is Needed* (GAO-14-103). The EPA prepared this response pursuant to 31 U.S.C. 720.

The agency appreciates the GAO's acknowledgment that the EPA has effectively addressed recommendations from its prior report on this subject, *Safe Drinking Water: EPA Should Improve Implementation of Requirements on Whether to Regulate Additional Contaminants* (GAO-11-254). The EPA generally agrees with the GAO's "Recommendations for Executive Action" and we plan to address those recommendations as described below.

GAO Recommendation

The Administrator of the Environmental Protection Agency should direct the Assistant Administrator of the Office of Water to help ensure that the UCMR [Unregulated Contaminant Monitoring Rule] data accurately reflect contaminant occurrence, vary the monitoring frequency for public water systems when the standard UCMR monitoring frequency is not expected to accurately detect the presence of contaminants, such as sporadically occurring viruses or pesticides that fluctuate seasonally.

EPA Response

Beginning with the development of the rule for the next UCMR cycle ("UCMR 4"), the EPA will give greater consideration to the potential for particular contaminants to occur sporadically and/or seasonally. To the extent practical, taking into account factors such as cost and implementation considerations, the agency will seek to adjust the monitoring frequency for contaminants that are anticipated to have significant sporadic and/or seasonal occurrence.

GAO Recommendation

The Administrator of the Environmental Protection Agency should direct the Assistant Administrator of the Office of Water to help address potential limitations with the UCMR data, when considering if adequate data had been collected under a prior UCMR during the contaminant selection process, take

into account whether: (1) the sampling methodology EPA used in a prior UCMR for a particular contaminant provided sufficient occurrence data to make a regulatory determination, (2) the contaminant's health information is in flux or has been updated and now indicates that adverse health effects occur at a lower level than that at which UCMR data were originally collected, or (3) the data collected in an earlier cycle have become outdated and no longer present an accurate picture of contaminant occurrence, for example, because industrial or agricultural chemical use has changed.

EPA Response

Beginning with the development of the rule for UCMR 4, the EPA will give greater consideration to whether additional occurrence data gathering is warranted for contaminants monitored during prior UCMR cycles. The agency will specifically consider (1) the sampling methodology used in the prior cycle; (2) changes in health information (e.g., establishment of a lower health reference level) that may warrant additional monitoring at a lower level; and (3) the degree to which the available data are expected to be representative of current contaminant occurrence. These factors will be considered in the agency's establishment of relative priorities for UCMR contaminant selection. As to the use of the UCMR data from prior cycles to support the agency's regulatory determinations, the EPA will continue to judge the appropriateness of the data on a case-by-case basis. As acknowledged in the report, the agency uses the "best available" data to support its decisions.

GAO Recommendation

The Administrator of the Environmental Protection Agency should direct the Assistant Administrator of the Office of Water to optimize the ability of the UCMR program to support regulatory determinations, convene an internal working group of officials responsible for the UCMR, regulatory determinations, and CCL [Contaminant Candidate List] to fully examine opportunities to improve the timeliness of the UCMR program. Among other things, the working group should consider: (1) whether a shorter process for selecting contaminants would yield a high-quality list, or whether the existing process can be started sooner, and (2) whether monitoring for contaminants over a shorter period, instead of the current 3-year period, is feasible, given data quality, logistical needs, and the burden on public water systems.

EPA Response

The EPA will convene the recommended workgroup and will consider, among the potential improvements, the practicality of a shorter process for contaminant selection and a shorter period for contaminant monitoring. Workgroup recommendations will be incorporated into our approach to the extent practical.

The EPA expresses its appreciation for the thoughtful work and professionalism of the GAO staff members throughout this review. If you have any further questions, please contact me or your staff may contact Christina Moody in the EPA's Office of Congressional and Intergovernmental Relations, by phone at (202) 564-0260, or by email at moody.christina@epa.gov.

Sincerely,

Maryann Froehlich
Acting Chief Financial Officer

UNITED STATES ENVIRONMENTAL PROTECTION AGENCY
WASHINGTON, D.C. 20460

MAY - 9 2014

OFFICE OF THE
CHIEF FINANCIAL OFFICER

The Honorable Darrell Issa
Chairman
Committee on Oversight and Government Reform
U.S. House of Representatives
Washington, D.C. 20515

Dear Mr. Chairman:

I am transmitting the U.S. Environmental Protection Agency's response to the January 2014 Government Accountability Office report entitled, *EPA has Improved its Unregulated Contaminant Monitoring Program, but Additional Action is Needed* (GAO-14-103). The EPA prepared this response pursuant to 31 U.S.C. 720.

The agency appreciates the GAO's acknowledgment that the EPA has effectively addressed recommendations from its prior report on this subject, *Safe Drinking Water: EPA Should Improve Implementation of Requirements on Whether to Regulate Additional Contaminants* (GAO-11-254). The EPA generally agrees with the GAO's "Recommendations for Executive Action" and we plan to address those recommendations as described below.

GAO Recommendation

The Administrator of the Environmental Protection Agency should direct the Assistant Administrator of the Office of Water to help ensure that the UCMR [Unregulated Contaminant Monitoring Rule] data accurately reflect contaminant occurrence, vary the monitoring frequency for public water systems when the standard UCMR monitoring frequency is not expected to accurately detect the presence of contaminants, such as sporadically occurring viruses or pesticides that fluctuate seasonally.

EPA Response

Beginning with the development of the rule for the next UCMR cycle ("UCMR 4"), the EPA will give greater consideration to the potential for particular contaminants to occur sporadically and/or seasonally. To the extent practical, taking into account factors such as cost and implementation considerations, the agency will seek to adjust the monitoring frequency for contaminants that are anticipated to have significant sporadic and/or seasonal occurrence.

GAO Recommendation

The Administrator of the Environmental Protection Agency should direct the Assistant Administrator of the Office of Water to help address potential limitations with the UCMR data, when considering if adequate data had been collected under a prior UCMR during the contaminant selection process, take

into account whether: (1) the sampling methodology EPA used in a prior UCMR for a particular contaminant provided sufficient occurrence data to make a regulatory determination, (2) the contaminant's health information is in flux or has been updated and now indicates that adverse health effects occur at a lower level than that at which UCMR data were originally collected, or (3) the data collected in an earlier cycle have become outdated and no longer present an accurate picture of contaminant occurrence, for example, because industrial or agricultural chemical use has changed.

EPA Response

Beginning with the development of the rule for UCMR 4, the EPA will give greater consideration to whether additional occurrence data gathering is warranted for contaminants monitored during prior UCMR cycles. The agency will specifically consider (1) the sampling methodology used in the prior cycle; (2) changes in health information (e.g., establishment of a lower health reference level) that may warrant additional monitoring at a lower level; and (3) the degree to which the available data are expected to be representative of current contaminant occurrence. These factors will be considered in the agency's establishment of relative priorities for UCMR contaminant selection. As to the use of the UCMR data from prior cycles to support the agency's regulatory determinations, the EPA will continue to judge the appropriateness of the data on a case-by-case basis. As acknowledged in the report, the agency uses the "best available" data to support its decisions.

GAO Recommendation

The Administrator of the Environmental Protection Agency should direct the Assistant Administrator of the Office of Water to optimize the ability of the UCMR program to support regulatory determinations, convene an internal working group of officials responsible for the UCMR, regulatory determinations, and CCL [Contaminant Candidate List] to fully examine opportunities to improve the timeliness of the UCMR program. Among other things, the working group should consider: (1) whether a shorter process for selecting contaminants would yield a high-quality list, or whether the existing process can be started sooner, and (2) whether monitoring for contaminants over a shorter period, instead of the current 3-year period, is feasible, given data quality, logistical needs, and the burden on public water systems.

EPA Response

The EPA will convene the recommended workgroup and will consider, among the potential improvements, the practicality of a shorter process for contaminant selection and a shorter period for contaminant monitoring. Workgroup recommendations will be incorporated into our approach to the extent practical.

The EPA expresses its appreciation for the thoughtful work and professionalism of the GAO staff members throughout this review. If you have any further questions, please contact me or your staff may contact Christina Moody in the EPA's Office of Congressional and Intergovernmental Relations, by phone at (202) 564-0260, or by email at moody.christina@epa.gov.

Sincerely,

Maryann Froehlich
Acting Chief Financial Officer

UNITED STATES ENVIRONMENTAL PROTECTION AGENCY
WASHINGTON, D.C. 20460

MAY - 9 2014

OFFICE OF THE
CHIEF FINANCIAL OFFICER

The Honorable Barbara A. Mikulski
Chairwoman
Committee on Appropriations
United States Senate
Washington, D.C. 20510

Dear Madam Chairwoman:

I am transmitting the U.S. Environmental Protection Agency's response to the January 2014 Government Accountability Office report entitled, *EPA has Improved its Unregulated Contaminant Monitoring Program, but Additional Action is Needed* (GAO-14-103). The EPA prepared this response pursuant to 31 U.S.C. 720.

The agency appreciates the GAO's acknowledgment that the EPA has effectively addressed recommendations from its prior report on this subject, *Safe Drinking Water: EPA Should Improve Implementation of Requirements on Whether to Regulate Additional Contaminants* (GAO-11-254). The EPA generally agrees with the GAO's "Recommendations for Executive Action" and we plan to address those recommendations as described below.

GAO Recommendation

The Administrator of the Environmental Protection Agency should direct the Assistant Administrator of the Office of Water to help ensure that the UCMR [Unregulated Contaminant Monitoring Rule] data accurately reflect contaminant occurrence, vary the monitoring frequency for public water systems when the standard UCMR monitoring frequency is not expected to accurately detect the presence of contaminants, such as sporadically occurring viruses or pesticides that fluctuate seasonally.

EPA Response

Beginning with the development of the rule for the next UCMR cycle ("UCMR 4"), the EPA will give greater consideration to the potential for particular contaminants to occur sporadically and/or seasonally. To the extent practical, taking into account factors such as cost and implementation considerations, the agency will seek to adjust the monitoring frequency for contaminants that are anticipated to have significant sporadic and/or seasonal occurrence.

GAO Recommendation

The Administrator of the Environmental Protection Agency should direct the Assistant Administrator of the Office of Water to help address potential limitations with the UCMR data, when considering if adequate data had been collected under a prior UCMR during the contaminant selection process, take

into account whether: (1) the sampling methodology EPA used in a prior UCMR for a particular contaminant provided sufficient occurrence data to make a regulatory determination, (2) the contaminant's health information is in flux or has been updated and now indicates that adverse health effects occur at a lower level than that at which UCMR data were originally collected, or (3) the data collected in an earlier cycle have become outdated and no longer present an accurate picture of contaminant occurrence, for example, because industrial or agricultural chemical use has changed.

EPA Response

Beginning with the development of the rule for UCMR 4, the EPA will give greater consideration to whether additional occurrence data gathering is warranted for contaminants monitored during prior UCMR cycles. The agency will specifically consider (1) the sampling methodology used in the prior cycle; (2) changes in health information (e.g., establishment of a lower health reference level) that may warrant additional monitoring at a lower level; and (3) the degree to which the available data are expected to be representative of current contaminant occurrence. These factors will be considered in the agency's establishment of relative priorities for UCMR contaminant selection. As to the use of the UCMR data from prior cycles to support the agency's regulatory determinations, the EPA will continue to judge the appropriateness of the data on a case-by-case basis. As acknowledged in the report, the agency uses the "best available" data to support its decisions.

GAO Recommendation

The Administrator of the Environmental Protection Agency should direct the Assistant Administrator of the Office of Water to optimize the ability of the UCMR program to support regulatory determinations, convene an internal working group of officials responsible for the UCMR, regulatory determinations, and CCL [Contaminant Candidate List] to fully examine opportunities to improve the timeliness of the UCMR program. Among other things, the working group should consider: (1) whether a shorter process for selecting contaminants would yield a high-quality list, or whether the existing process can be started sooner, and (2) whether monitoring for contaminants over a shorter period, instead of the current 3-year period, is feasible, given data quality, logistical needs, and the burden on public water systems.

EPA Response

The EPA will convene the recommended workgroup and will consider, among the potential improvements, the practicality of a shorter process for contaminant selection and a shorter period for contaminant monitoring. Workgroup recommendations will be incorporated into our approach to the extent practical.

The EPA expresses its appreciation for the thoughtful work and professionalism of the GAO staff members throughout this review. If you have any further questions, please contact me or your staff may contact Christina Moody in the EPA's Office of Congressional and Intergovernmental Relations, by phone at (202) 564-0260, or by email at moody.christina@epa.gov.

Sincerely,

Maryann Froehlich
Acting Chief Financial Officer

UNITED STATES ENVIRONMENTAL PROTECTION AGENCY
WASHINGTON, D.C. 20460

MAY - 9 2014

OFFICE OF THE
CHIEF FINANCIAL OFFICER

The Honorable Eugene Dodaro
Comptroller General
Government Accountability Office
Washington, D.C. 20548

Dear Mr. Dodaro:

I am transmitting to you the U.S. Environmental Protection Agency's responses to the recommendations set forth in the Government Accountability Office report entitled, *EPA has Improved its Unregulated Contaminant Monitoring Program, but Additional Action is Needed* (GAO-14-103). The EPA prepared this response pursuant to 31 U.S.C. 720.

The agency reviewed the report and pursuant to 31 U.S.C. 720, enclosed are copies of the EPA responses to the Chairs of the House Committee on Oversight and Government Reform, the Senate Committee on Homeland Security and Governmental Affairs, and the House and Senate Committees on Appropriations. If you have any further questions, please contact me or your staff may contact Christina Moody in the EPA's Office of Congressional and Intergovernmental Relations, by phone at (202) 564-0260 or by email at moody.christina@epa.gov.

Sincerely,

Maryann Froehlich

Maryann Froehlich
Acting Chief Financial Officer

Enclosures

UNITED STATES ENVIRONMENTAL PROTECTION AGENCY
WASHINGTON, D.C. 20460

MAY - 9 2014

OFFICE OF THE
CHIEF FINANCIAL OFFICER

The Honorable Sylvia M. Burwell
Director
Office of Management and Budget
Washington, D.C. 20503

Dear Ms. Burwell:

I am transmitting to you the U.S. Environmental Protection Agency's responses to the recommendations set forth in the Government Accountability Office report entitled, *EPA has Improved its Unregulated Contaminant Monitoring Program, but Additional Action is Needed* (GAO-14-103). The EPA prepared this response pursuant to 31 U.S.C. 720.

The agency reviewed the report and pursuant to 31 U.S.C. 720, enclosed are copies of the EPA responses to the Chairs of the House Committee on Oversight and Government Reform, the Senate Committee on Homeland Security and Governmental Affairs, and the House and Senate Committees on Appropriations. If you have any further questions, please contact me or your staff may contact Christina Moody in the EPA's Office of Congressional and Intergovernmental Relations, by phone at (202) 564-0260 or by email at moody.christina@epa.gov.

Sincerely,

Maryann Froehlich

Maryann Froehlich
Acting Chief Financial Officer

Enclosures

OAL 14-001-1556

UNITED STATES ENVIRONMENTAL PROTECTION AGENCY
WASHINGTON, D.C. 20460

SEP 29 2014

OFFICE OF THE
CHIEF FINANCIAL OFFICER

The Honorable Harold Rogers
Chairman
Committee on Appropriations
U.S. House of Representatives
Washington, D.C. 20515

Dear Mr. Chairman:

I am transmitting the U.S. Environmental Protection Agency's response to the December 2013 Government Accountability Office report entitled, *Clean Water Act: Changes Needed if Key EPA Program is to Help Fulfill the Nation's Water Quality Goals* (GAO-14-80). The EPA prepared this response pursuant to 31 U.S.C. 720.

The EPA generally agrees with the GAO's findings. The agency agrees with the report's characterization of the challenges facing the EPA's water quality-based programs (i.e., the broader context within which the Total Maximum Daily Load program operates) under the Clean Water Act. The GAO thoroughly analyzed and understands the abundance and complexity of impaired waters across the nation, the limited funding and authorities for the EPA and our state partners under the CWA programs, and the limited achievement of the CWA goals to date. The EPA commends the GAO's substantial investment of effort in designing and carrying out a statistical survey of state water quality managers that has contributed new empirical data and insights into state TMDL development and implementation, including some findings on impaired waters restoration status and outcomes.

A summary of the EPA's response to each of the report's recommendations follows.

GAO Recommendation

To enhance the likelihood that TMDLs support the nation's waters' attainment of water quality standards and to strengthen water quality management, the Administrator of EPA should develop and issue new regulations requiring that TMDLs include additional elements--and consider requiring the elements that are now optional--specifically, elements reflecting key features identified by NRC [the National Research Council] as necessary for attaining water quality standards, such as comprehensive identification of impairment and plans to monitor water bodies to verify that water quality is improving.

EPA Response:

The EPA is not planning to issue broad new TMDL regulations at this time. Instead, to help address this recommendation, the EPA plans to continue its long-standing promotion of comprehensive watershed management well beyond the TMDL program.

GAO Recommendation

To enhance the likelihood that TMDLs support the nation's waters' attainment of water quality standards and to strengthen water quality management, the Administrator of EPA should ensure more consistent application of existing TMDL elements and to provide greater assurance that TMDLs, if implemented, can achieve tangible water quality results, identify regional offices with criteria for interpreting and applying such elements in reviewing and approving state-developed TMDLs and issue guidance with more specificity, directing all regional offices to follow the same criteria, including requesting that states provide more-detailed information about pollution causes and abatement actions.

EPA Response

The EPA agrees with this recommendation. We see national coordination and guidance on procedures for the EPA regional TMDL review and approval as an ongoing responsibility. We consistently maintain dialogue across the regional TMDL programs via monthly conference calls that frequently include specific case studies or TMDL approval issues. We plan to initiate a dialogue with our regional offices on the overall TMDL review and approval guidance during calendar years 2014-2015; this dialogue will consider the GAO's recommended changes.

GAO Recommendation

To enhance the likelihood that TMDLs support the nation's waters' attainment of water quality standards and to strengthen water quality management, the Administrator of EPA should place conditions on states' annual use of nonpoint source management and water pollution control grants to ensure that the funds meet the purposes for which they are awarded and achieve greater reductions in nonpoint source pollution associated with TMDL implementation, such as by targeting funds to states and projects that incorporate factors needed for effective TMDL implementation (e.g., targeting grant funds to projects where implementation plans have been developed and where external agency assistance is available).

EPA Response

The agency agrees with this recommendation. In the Section 319 program, we require nine-element watershed plans before these funds are spent on watershed restoration projects, including those funds that implement the TMDLs. In April 2013, the EPA's Non-Point Source Control Program reissued the Section 319 guidance, with several modifications that strengthen the TMDL-related implementation and on-the-ground control actions. Among the provisions in the new guidance were several elements related to the GAO's recommendation, in particular "an increased emphasis on watershed project implementation in watersheds with impaired waters, and greater accountability measures." More emphasis is placed on watershed implementation by requiring a full 50 percent of the Section 319 funds to go for that purpose. The guidance also requires supplemental information for the TMDLs developed with the Section 319 funds, including detailed identification of causes/sources, existing loads and load reductions needed by source, and management measures to achieve load reduction. These improvements are in the form of a Section 319 grant condition, not a new TMDL element, and are structured to make the TMDLs more useful to watershed based plans and vice versa.

The EPA agrees to review the possible uses of Section 106 funding to address this recommendation, as Section 106 funds frequently support the development of TMDLs. We will share this recommendation with other sources of funding, including geographic programs such as the Great Lakes Restoration Initiative and the Chesapeake Bay Program.

GAO Recommendation

To enhance the likelihood that TMDLs support the nation's waters' attainment of water quality standards and to strengthen water quality management, the Administrator of EPA should obtain missing data that currently impede EPA's efforts to determine whether and to what extent TMDLs have been implemented or to what extent implemented TMDLs have helped impaired waters attain water quality standards by (1) directing states to use and report specific Geographic Information Systems data when implementing projects to which TMDLs apply and (2) requesting that USDA [the United States Department of Agriculture] ask landowners who participate in conservation programs funded by the Department in areas subject to a TMDL to disclose information on the location, type, and number of projects implemented under these programs.

EPA Response

The EPA generally agrees with the first part of this recommendation. The EPA agrees that geospatial data provides a highly valuable basis for data integration from multiple information sources. Permits and Section 319 tracking continue to accumulate geo-referenced information for newer permits and projects. In 2013, the EPA actively engaged with states on a study of geospatial data requirements and applications that seeks to provide greater efficiencies in impaired waters and the TMDL reporting and data management. We expect this project and a broader effort on an improved, national EPA geospatial framework to remain a priority activity during calendar year 2014 and beyond.

On the second part, we have shared the recommendation with the USDA and suggest the GAO might also apprise the USDA of this request.

The EPA expresses its appreciation for the thoughtful work of the GAO staff members throughout this review and their engagement with staff at the EPA headquarters and regions, as well as at the state water program levels. If you have any further questions, please contact me or your staff may contact Christina Moody in the EPA's Office of Congressional and Intergovernmental Relations, by phone at (202) 564-0260, or by email at moody.christina@epa.gov.

Sincerely,

David Bloom
Acting Chief Financial Officer

AL 14-001-4190

THE ADMINISTRATOR OF THE ENVIRONMENTAL PROTECTION AGENCY

WASHINGTON, D.C. 20460

AUG 22 2014

The Honorable Harold Rogers
Chairman
Committee on Appropriations
U.S. House of Representatives
Washington, DC 20515

Dear Mr. Chairman:

I am pleased to support the charter National Advisory Committee to the United States Representative to the North American Commission for Environmental Cooperation in accordance with the provisions of the Federal Advisory Committee Act, 5 U.S.C. App. 2. The National Advisory Committee to the United States Representative to the North American Commission for Environmental Cooperation is in the public interest and supports the U.S. Environmental Protection Agency in performing its duties and responsibilities.

I am filing the enclosed charter with the Library of Congress. The National Advisory Committee to the United States Representative to the North American Commission for Environmental Cooperation will be in effect for two years from the date the charter is filed with Congress. After two years, the charter may be renewed as authorized in accordance with Section 14 of FACA (5 U.S.C. App. 2 § 14).

If you have any questions or require additional information, please contact me or your staff may contact Christina Moody in EPA's Office of Congressional and Intergovernmental Relations at Moody.christina@epa.gov or (202) 564-0260.

Sincerely,

Gina McCarthy

Enclosure

14-001-4190

UNITED STATES ENVIRONMENTAL PROTECTION AGENCY CHARTER

NATIONAL ADVISORY COMMITTEE TO THE UNITED STATES REPRESENTATIVE TO THE NORTH AMERICAN COMMISSION FOR ENVIRONMENTAL COOPERATION

1. Committee's Official Designation (Title):

National Advisory Committee to the United States Representative to the North American Commission for Environmental Cooperation

2. Authority:

This charter renews the National Advisory Committee (NAC) to the United States Representative to the Council of the Commission for Environmental Cooperation (CEC) in accordance with the provisions of the Federal Advisory Committee Act (FACA), 5 U.S.C. App. 2. The NAC is in the public interest and advises the U.S. Representative on implementation and elaboration of the North American Agreement on Environmental Cooperation (NAAEC). Establishment of the committee is authorized under article 17 of the NAAEC and by the North American Free Trade Agreement Implementation Act, P.L. 103-182, which authorizes U.S. participation in the CEC. Federal government responsibilities relating to the committee are set forth in Executive Order 12915, entitled "Federal Implementation of the North American Agreement on Environmental Cooperation."

3. Objectives and Scope of Activities:

The NAC will provide advice, information and recommendations on a broad range of environment-related strategic, scientific, technological, regulatory and economic issues to be addressed in implementation and elaboration of the NAAEC.

4. Description of Committee's Duties:

The duties of the NAC are solely to provide advice to EPA.

5. Official(s) to Whom the Committee Reports:

The NAC will submit advice and recommendations and report to the Environmental Protection Agency (EPA) Administrator, who serves as the United States Representative to the Council of the CEC under the authority of Executive Order 12915.

6. **Agency Responsible for Providing the Necessary Support:**

EPA will be responsible for financial and administrative support. Within EPA, this support will be provided by the Office of Diversity, Advisory Committee Management and Outreach, within the Office of Administration and Resources Management.

7. **Estimated Annual Operating Costs and Work Years:**

The estimated annual operating cost of the NAC is $166,000 which includes 0.7 person-years of support.

8. **Designated Federal Officer:**

A full-time or permanent part-time employee of EPA will be appointed as the Designated Federal Officer (DFO). The DFO or a designee will be present at all meetings of the advisory committee and subcommittees. Each meeting will be conducted in accordance with an agenda approved in advance by the DFO. The DFO is authorized to adjourn any meeting when he or she determines it is in the public interest to do so, and will chair meetings when directed to do so by the official to whom the committee reports.

9. **Estimated Number and Frequency of Meetings:**

The NAC expects to meet approximately three (3) times a year. Meetings may occur approximately once every four (4) months or as needed and approved by the DFO. EPA may pay travel and per diem expenses when determined necessary and appropriate.

As required by FACA, the NAC will hold open meetings unless the EPA Administrator determines that a meeting or a portion of a meeting may be closed to the public in accordance with 5 U.S.C. 552b(c). Interested persons may attend meetings, appear before the committee as time permits, and file comments with the NAC.

10. **Duration and Termination:**

This charter will be in effect for two years from the date it is filed with Congress. After this two-year period, the charter may be renewed as authorized in accordance with Section 14 of FACA.

11. **Member Composition:**

The NAC will be composed of approximately fifteen (15) members who will serve as Representative members of non-federal interests, Regular Government Employees (RGEs), or Special Government Employees (SGEs). Representative members are selected to represent the points of view held by organizations, associations, or classes of individuals. In selecting members, EPA will consider candidates from the following stakeholder categories: environmental groups and non-profit entities, business and industry, and educational institutions.

14-001-4190

12. **Subgroups:**

EPA, or the NAC with EPA approval, may form NAC subcommittees or workgroups for any purpose consistent with this charter. Such subcommittees or workgroups may not work independently of the chartered committee and must report their recommendations and advice to the chartered NAC for full deliberation and discussion. Subcommittees or workgroups have no authority to make decisions on behalf of the chartered committee nor can they report directly to the U.S. Representative to the Council of the CEC.

13. **Recordkeeping:**

The records of the committee, formally and informally established subcommittees, or other subgroups of the committee, will be handled in accordance with NARA General Records Schedule 26, Item 2 and EPA Records Schedule 181 or other approved agency records disposition schedule. Subject to the Freedom of Information Act, 5 U.S.C. 552, these records will be available for public inspection and copying, in accordance with the Federal Advisory Committee Act.

JUL 29 2014

Agency Approval Date

AUG 22 2014

Date Filed with Congress

AL 14-001-4639

THE ADMINISTRATOR OF THE ENVIRONMENTAL PROTECTION AGENCY

WASHINGTON, D.C. 20460

SEP 05 2014

The Honorable Harold Rogers
Chairman
Committee on Appropriations
U.S. House of Representatives
Washington, DC 20515

Dear Mr. Chairman:

I am pleased to support the charter Good Neighbor Environmental Board in accordance with the provisions of the Federal Advisory Committee Act, 5 U.S.C. App. 2. The Good Neighbor Environmental Board is in the public interest and supports the U.S. Environmental Protection Agency in performing its duties and responsibilities.

I am filing the enclosed charter with the Library of Congress. The Good Neighbor Environmental Board will be in effect for two years from the date the charter is filed with Congress. After two years, the charter may be renewed as authorized in accordance with Section 14 of FACA (5 U.S.C. App. 2 § 14).

If you have any questions or require additional information, please contact me or your staff may contact Christina Moody in EPA's Office of Congressional and Intergovernmental Relations at Moody.christina@epa.gov or (202) 564-0260.

Sincerely,

Gina McCarthy

Enclosure

JAL 14-001-5252

THE ADMINISTRATOR OF THE ENVIRONMENTAL PROTECTION AGENCY

WASHINGTON, D.C. 20460

SEP 12 2014

The Honorable Harold Rogers
Chairman
Committee on Appropriations
U.S. House of Representatives
Washington, DC 20515

Dear Mr. Chairman:

I am pleased to support the charter National Environmental Justice Advisory Council in accordance with the provisions of the Federal Advisory Committee Act, 5 U.S.C. App. 2. The National Environmental Justice Advisory Council is in the public interest and supports the U.S. Environmental Protection Agency in performing its duties and responsibilities.

I am filing the enclosed charter with the Library of Congress. The National Environmental Justice Advisory Council will be in effect for two years from the date the charter is filed with Congress. After two years, the charter may be renewed as authorized in accordance with Section 14 of FACA (5 U.S.C. App. 2 § 14).

If you have any questions or require additional information, please contact me or your staff may contact Christina Moody in EPA's Office of Congressional and Intergovernmental Relations at Moody.christina@epa.gov or (202) 564-0260.

Sincerely,

Gina McCarthy

Enclosure

14-001-5252

UNITED STATES ENVIRONMENTAL PROTECTION AGENCY CHARTER

NATIONAL ENVIRONMENTAL JUSTICE ADVISORY COUNCIL

1. Committee's Official Designation (Title):

National Environmental Justice Advisory Council

2. Authority:

This charter renews the National Environmental Justice Advisory Council (NEJAC) in accordance with the requirements of the Federal Advisory Committee Act (FACA), 5 U.S.C. App. 2. The NEJAC is in the public interest and supports the Environmental Protection Agency (EPA) in performing its duties and responsibilities.

3. Objectives and Scope of Activities:

The NEJAC will provide independent advice and recommendations to the Administrator about broad, crosscutting issues related to environmental justice. The NEJAC's efforts will include evaluation of a broad range of strategic, scientific, technological, regulatory, community engagement and economic issues related to environmental justice. The major objectives will be to provide advice and recommendations about EPA efforts to:

a. Integrate environmental justice considerations into Agency programs, policies and activities
b. Improve the environment or public health in communities disproportionately burdened by environmental harms and risks
c. Address environmental justice to ensure meaningful involvement in EPA decision-making, build capacity in disproportionately-burdened communities, and promote collaborative problem-solving for issues involving environmental justice
d. Strengthen its partnerships with other governmental agencies, such as other Federal agencies and state, tribal, or local governments, regarding environmental justice issues
e. Enhance research and assessment approaches related to environmental justice

4. Description of Committees Duties:

The duties of the NEJAC are solely to advise the EPA.

5. Official(s) to Whom the Committee Reports:

The NEJAC will provide advice and recommendations, and report to the EPA Administrator through the Office of Environmental Justice, Office of Enforcement and Compliance Assurance.

6. **Agency Responsible for Providing the Necessary Support:**

EPA will be responsible for financial and administrative support. Within EPA, this support will be provided by the Office of Environmental Justice, Office of Enforcement and Compliance Assurance.

7. **Estimated Annual Operating Costs and Work Years:**

The estimated annual operating cost of the NEJAC is $295,600, which includes 1.5 person-years of support.

8. **Designated Federal Officer:**

A full-time or permanent part-time employee of EPA will be appointed as the Designated Federal Officer (DFO). The DFO or a designee will be present at all of the meetings of the advisory committee and subcommittees. Each meeting will be conducted in accordance with an agenda approved in advance by the DFO. The DFO is authorized to adjourn any meeting when he or she determines it is in the public interest to do so, and will chair meetings when directed to do so by the official to whom the committee reports.

9. **Estimated Number and Frequency of Meetings:**

The NEJAC expects to meet approximately two (2) to four (4) times a year. Meetings may occur approximately once every three to six months, as needed and approved by the Designated Federal Officer (DFO), or his/her designee. EPA may pay travel and per diem expenses when determined necessary and appropriate.

As required by FACA, the NEJAC will hold open meetings, unless the EPA Administrator determines that a meeting or a portion of a meeting may be closed to the public in accordance with 5 U.S.C. 552b(c). Interested persons may attend meetings, appear before the committee as time permits, and file comments with the NEJAC.

10. **Duration and Termination:**

The NEJAC will be examined annually and will exist until the EPA determines the Council is no longer needed. This charter will be in effect for two years from the date it is filed with Congress. After this two-year period, the charter may be renewed in accordance with Section 14 of FACA.

14-001-5252

11. **Member Composition:**

The NEJAC will be composed of approximately 27 members who will serve as Representative members of non-federal interests, Regular Government Employees (RGE), or Special Government Employees (SGE). Representative members are selected to represent the points of view held by organizations, associations, or classes of individuals. In selecting members, EPA will consider candidates from among, but not limited to: community-based groups; industry and business; academic and educational institutions; state and local governments; indigenous organization and Federally-recognized tribal governments and Indigenous groups; and non-governmental and environmental groups, as deemed appropriate.

12. **Subgroups:**

EPA, or the NEJAC with EPA approval, may form subcommittees or work groups for any purpose consistent with this charter. Such subcommittees or work groups may not work independently of the chartered committee and must report their proposed recommendations and advice to the chartered NEJAC for full deliberation and discussion. Subcommittees or work groups have no authority to make decisions on behalf of the chartered committee nor can they report directly to the EPA.

13. **Recordkeeping:**

The records of the committee, formally and informally established subcommittees, or other subgroups of the committee, will be handled in accordance with NARA General Records Schedule 26, Item 2 and EPA Records Schedule 181 or other approved agency records disposition schedule. Subject to the Freedom of Information Act, 5 U.S.C. 552, these records will be available for public inspection and copying, in accordance with the Federal Advisory Committee Act.

8/8/2014
Agency Approval Date

AUG 20 2014
GSA Consultation Date

SEP 12 2014
Date Filed with Congress

AL12-000-8215

UNITED STATES ENVIRONMENTAL PROTECTION AGENCY
WASHINGTON, D.C. 20460

MAY 18 2012

OFFICE OF THE
CHIEF FINANCIAL OFFICER

The Honorable Harold Rogers
Chairman
Committee on Appropriations
U.S. House of Representatives
Washington, D.C. 20515

Dear Mr. Chairman:

I am transmitting the U.S. Environmental Protection Agency's response to the February 2012 Government Accountability Office report entitled, *Electronic Waste: Actions Needed to Provide Assurance that Used Federal Electronics are Disposed of in an Environmentally Responsible Manner* (GAO-12-74). The EPA prepared this response pursuant to 31 U.S.C. 720.

To improve federal electronics stewardship, the GAO made four recommendations, one directed towards the Administrator of the EPA.

GAO Recommendation

To provide transparency on progress toward completing the actions identified in the National Strategy for Electronics Stewardship, we recommend that the Director of CEQ, the Administrator of EPA, and the Administrator of GSA provide quarterly status updates on a publically accessible website.

EPA Response

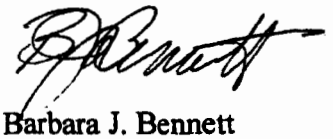
The agency would like to reiterate our previous request made to the GAO for one slight revision to the recommendation. The EPA plans to update its progress at least twice a year. We believe that being transparent to the public on progress being made in implementing these projects is paramount. These beliefs were discussed among the three agencies (the Environmental Protection Agency, the General Services Administration, and the Council on Environmental Quality) at length prior to the release of the National Strategy for Electronics Stewardship. Specific language was carefully negotiated among the participating agencies to reflect that the goals were targets not deadlines due to resource considerations that confront each of the agencies.

Due to the nature of some of the work we have committed to (i.e., planning, information gathering, and tool development) and length of time needed to make reasonable progress, it is more appropriate to report progress to the public at least twice a year, rather than on a strict quarterly schedule. In addition, each project will arrive at a key milestone or a public announcement at different points. Many projects require input from stakeholders to ensure that the finished project results in a completely informed and robust effort. Furthermore, we are planning public events for some projects.

Based on these reasons, we plan to update the publically available website at least twice a year as we make significant progress and/or as we meet key milestones on the projects.

Thank you for the opportunity to respond to this recommendation. Overall, we are pleased with the positive portrayal of the programs that the EPA has a hand in developing and/or implementing. If you have any questions, please contact me or your staff may call Christina Moody, in the EPA's Office of Congressional and Intergovernmental Relations, at (202) 564-0260.

Sincerely,



Barbara J. Bennett
Chief Financial Officer

AL 12-000-8300

UNITED STATES ENVIRONMENTAL PROTECTION AGENCY
WASHINGTON, D.C. 20460

MAY 1 1 2012

THE ADMINISTRATOR

The Honorable Harold Rogers
Chairman
Committee on Appropriations
U.S. House of Representatives
Washington, DC 20515

Dear Mr. Chairman:

I am pleased to renew the EPA Board of Scientific Counselors in accordance with the provisions of the Federal Advisory Committee Act, 5 U.S.C. App. 2. The EPA Board of Scientific Counselors is in the public interest and supports the U.S. Environmental Protection Agency in performing its duties and responsibilities.

I am filing the enclosed charter with the Library of Congress. The EPA Board of Scientific Counselors will be in effect for two years from the date the charter is filed with Congress. After two years, the charter may be renewed as authorized in accordance with Section 14 of FACA (5 U.S.C. App. 2 § 14).

If you have any questions or require additional information, please contact me or your staff may contact Clara Jones in the EPA's Office of Congressional and Intergovernmental Relations at (202) 564-3701.

Sincerely,

Lisa P. Jackson

Enclosure

12-000-8300

UNITED STATES ENVIRONMENTAL PROTECTION AGENCY

EPA BOARD OF SCIENTIFIC COUNSELORS

---

1. **Committee's Official Designation (Title):**

EPA Board of Scientific Counselors

2. **Authority:**

The EPA Board of Scientific Counselors (BOSC) charter is renewed in accordance with the provisions of the Federal Advisory Committee Act (FACA), 5 U.S.C. App. 2. The BOSC is in the public interest and supports EPA in performing its duties and responsibilities.

3. **Objectives and Scope of Activities:**

The BOSC will provide advice and recommendations on all aspects (technical and management) of the Office of Research and Development's (ORD) research program. As appropriate, the BOSC will consult and coordinate its work with the Science Advisory Board.

The major objectives are to provide advice and recommendations on:

a. ORD's research programs and research-management practices, and to recommend actions to improve research program quality, relevance, and performance, as well as program structure, scientific leadership, coordination/communication, and outcomes;

b. ORD's program development, progress, and research program balance, which may include evaluation of multi-year plans and implementation of the ORD Strategic Plan;

c. Use of peer review within ORD to sustain and enhance the quality of science in EPA;

d. Scientific and management issues specific to ORD Offices, National Laboratories, and Centers; and

e. ORD's human resources planning, such as scientist career development and rotational assignment programs, and the appropriate scope and design of training programs for environmental research professionals.

4. **Description of Committees Duties:**

The duties of the BOSC are solely to provide policy advice to EPA.

5. **Official(s) to Whom the Committee Reports:**

The BOSC will submit advice and recommendations and report to the EPA Administrator, through the Assistant Administrator for the Office of Research and Development, in consultation with the Administrator's Science Advisor.

6. **Agency Responsible for Providing the Necessary Support:**

The EPA will be responsible for financial and administrative support. Within EPA, this support will be provided by the Office of Research and Development.

7. **Estimated Annual Operating Costs and Work Years:**

The estimated annual operating cost of the BOSC is $288,000 which includes 1.0 person-years of support.

8. **Designated Federal Officer:**

A full-time or permanent part-time employee of EPA will be appointed as the Designated Federal Officer (DFO). The DFO or a designee will be present at all of the advisory committee's and subcommittee's meetings. Each meeting will be conducted in accordance with an agenda approved in advance by the DFO. The DFO is authorized to adjourn any meeting when he or she determines it is in the public interest to do so, and will chair meetings when directed to do so by the official to whom the committee reports.

9. **Estimated Number and Frequency of Meetings:**

The BOSC expects to meet approximately two (2) to three (3) times a year. Meetings may occur approximately once every four (4) to six (6) months, or as needed and approved by the Designated Federal Officer (DFO). EPA may pay travel and per diem expenses when determined necessary and appropriate.

As required by FACA, the BOSC will hold open meetings unless the EPA Administrator determines that a meeting or a portion of a meeting may be closed to the public in accordance with subsection c of Section 552b of Title 5. Interested persons may attend meetings, appear before the committee as time permits, and file comments with the BOSC.

10. **Duration and Termination:**

The BOSC will be examined annually and will exist until the EPA determines the committee is no longer needed. This charter will be in effect for two years from the date it is filed with Congress. After the initial two-year period, the charter may be renewed as authorized in accordance with Section 14 of FACA.

12-000-8300

11. **Member Composition:**

The BOSC will be composed of approximately twenty (20) members who will serve as Special Government Employees (SGEs). In selecting members, EPA will consider candidates from the environmental scientific/technical fields, human health care professionals, academia, industry, public and private research institutes or organizations, and other relevant interest areas.

12. **Subgroups:**

The EPA, or the BOSC with EPA approval, may form BOSC subcommittees or workgroups for any purpose consistent with this charter. Such subcommittees or workgroups may not work independently of the chartered committee and must report their recommendations and advice to the BOSC for full deliberation and discussion. Subcommittees or workgroups have no authority to make decisions on behalf of the chartered committee nor can they report directly to the Agency.

13. **Recordkeeping:**

The records of the committee, formally and informally established subcommittees, or other subgroups of the committee, shall be handled in accordance with NARA General Records Schedule 26, Section 2 and EPA Records Schedule 181 or other approved agency records disposition schedule. Subject to the Freedom of Information Act, 5 U.S.C. 552, these records shall be available for public inspection and copying, in accordance with the Federal Advisory Committee Act.

May 7, 2012
Agency Approval Date

May 8, 2012
GSA Consultation Date

_____
Date Filed with Congress

AL 12-001-9581

UNITED STATES ENVIRONMENTAL PROTECTION AGENCY
WASHINGTON, D.C. 20460

DEC 13 2012

OFFICE OF THE
CHIEF FINANCIAL OFFICER

The Honorable Harold Rogers
Chairman
Committee on Appropriations
U.S. House of Representatives
Washington, D.C. 20515

Dear Mr. Chairman:

I am transmitting the U.S. Environmental Protection Agency's response to the September 2012 Government Accountability Office report entitled, *Organizational Transformation: Enterprise Architecture Value Needs to be Measured and Reported* (GAO-12-791). The EPA prepared this response pursuant to 31 U.S.C. 720.

GAO is making recommendations to the 27 federal agencies and OMB to improve measurement and reporting of architecture outcomes.

GAO Recommendations

To enhance federal agencies' ability to realize enterprise architecture benefits, we recommend the following actions.

We recommend that the Secretaries of the Departments of Agriculture, the Air Force, the Army, Commerce, Defense, Education, Energy, Homeland Security, the Interior, Labor, the Navy, State, Transportation, the Treasury, and Veterans Affairs; the Attorney General; the Administrators of the Environmental Protection Agency, General Services Administration, National Aeronautics and Space Administration, and Small Business Administration; the Commissioners of the Nuclear Regulatory Commission and Social Security Administration; and the Directors of the National Science Foundation and the Office of Personnel Management ensure the following two actions are taken:

- fully establish an approach for measuring enterprise architecture outcomes, including a documented method (i.e., steps to be followed) and metrics that are measurable, meaningful, repeatable, consistent, actionable, and aligned with the agency's enterprise architecture's strategic goals and intended purpose; and

- periodically measure and report enterprise architecture outcomes and benefits to top agency officials (i.e., executives with authority to commit resources or make changes to the program) and to OMB.

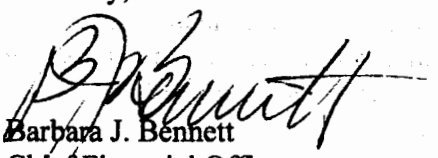
EPA Response

The EPA agrees with the GAO's comment that EPA has defined its architecture goals, objectives, and output metrics but needs to develop outcomes and benefits metrics. In recognition of the GAO's comment, the EPA plans to analyze the results of the enterprise architecture maturity self assessment to determine areas of improvement in performance management. In addition, the EPA review will include the Office of Management and Budget's planned December 2012 guidance for enterprise architecture value measurement and reporting.

The EPA will develop a performance measurement plan by September 2013. The plan will identify processes to measure enterprise architecture outcomes and benefits. The EPA will then periodically measure and report enterprise architecture outcomes and benefits to top agency officials and to the OMB in accordance with the GAO report recommendations for executive action.

Thank you for the opportunity to respond to these recommendations. We appreciate the information and detailed feedback provided by the GAO concerning areas addressed in this audit. If you have any questions, please contact me or your staff may call Christina Moody in the EPA's Office of Congressional and Intergovernmental Relations, at (202) 564-0260.

Sincerely,



Barbara J. Bennett
Chief Financial Officer

AL 12-002-0309

UNITED STATES ENVIRONMENTAL PROTECTION AGENCY
WASHINGTON, D.C. 20460

DEC 14 2012

THE ADMINISTRATOR

The Honorable Harold Rogers
Chairman
Committee on Appropriations
U.S. House of Representatives
Washington, DC 20515

Dear Mr. Chairman:

I am pleased to support the charter renewal of the National Drinking Water Advisory Council in accordance with the provisions of the Federal Advisory Committee Act, 5 U.S.C. App. 2. The National Drinking Water Advisory Council is in the public interest and supports the U.S. Environmental Protection Agency in performing its duties and responsibilities.

I am filing the enclosed charter with the Library of Congress. The Committee will be in effect for two years from the date it is filed with Congress. After two years, the charter may be renewed as authorized in accordance with Section 14 of FACA (5 U.S.C. App. 2 § 14).

If you have any questions or require additional information, please contact me or your staff may contact Christina J. Moody in EPA's Office of Congressional and Intergovernmental Relations at (202) 564-0260.

Sincerely,

Lisa P. Jackson

Enclosure

12-002-0369

UNITED STATES ENVIRONMENTAL PROTECTION AGENCY CHARTER

NATIONAL DRINKING WATER ADVISORY COUNCIL

1. Committee's Official Designation (Title):

National Drinking Water Advisory Council

2. Authority:

This charter renews the National Drinking Water Advisory Council (NDWAC or Council) in accordance with the provisions of the Federal Advisory Committee Act (FACA), 5 U.S.C. App.2. NDWAC is in the public interest and supports EPA in performing its duties and responsibilities. The Council was created by Congress on December 16, 1974, as part of the Safe Drinking Water Act of 1974, P.L. 93-523, 42 U.S.C. § 300j-5.

3. Objectives and Scope of Activities:

NDWAC will provide advice, information, and recommendations on matters related to activities, functions, policies, and regulations of the Environmental Protection Agency (EPA or Agency) under the Safe Drinking Water Act, including:

a. Providing practical and independent advice on matters and policies related to drinking water quality and public health protection.

b. Maintaining an awareness of developing issues and problems in the drinking water area and advising EPA on emerging issues.

c. Advising on regulations and guidance as required by the Safe Drinking Water Act.

d. Recommending policies with respect to the promulgation of drinking water standards.

e. Recommending special studies and research.

f. Assisting in identifying emerging environmental or health problems related to potentially hazardous constituents in drinking water.

g. Proposing actions to encourage cooperation and communication between EPA and other governmental agencies, interest groups, the general public, and technical associations and organizations on drinking water quality.

h. Analyzing sustainable infrastructure issues with special emphasis on the security of the nation's drinking water systems.

4. Description of Committees Duties:

The duties of NDWAC are to provide advice to EPA.

5. Official(s) to Whom the Committee Reports:

The NDWAC will report its advice and recommendations to the EPA Administrator.

6. Agency Responsible for Providing the Necessary Support:

EPA will be responsible for financial and administrative support. Within EPA, this support will be provided by the Office of Water.

7. Estimated Annual Operating Costs and Work Years:

The estimated annual operating cost of NDWAC is $252,000 which includes approximately 1.0 person-years of support.

8. Designated Federal Officer:

A full-time or permanent part-time employee of EPA will be appointed as the DFO. The DFO or a designee will be present at all of the advisory committee's and subcommittee meetings. Each meeting will be conducted in accordance with an agenda approved in advance by the DFO. The DFO is authorized to adjourn any meeting when he or she determines it is in the public interest to do so and will chair meetings when directed to do so by the official to whom the committee reports.

9. Estimated Number and Frequency of Meetings:

NDWAC expects to meet two (2) times a year. Meetings are expected to occur approximately once every six (6) months or as needed and approved by the Designated Federal Officer (DFO). As required by the Safe Drinking Water Act, EPA will pay members' travel and per diem expenses when members are "away from their homes or regular places of business in the performance of services for the Council." 42 U.S.C. § 300j-5(c).

As required by FACA, the Council will hold open meetings unless the EPA Administrator determines that a meeting or a portion of a meeting may be closed to the public in accordance with subsection c of the Government in the Sunshine Act, 5 U.S.C. § 552b. Interested persons may attend meetings, appear before the committee as time permits, and file comments with the NDWAC.

10. Duration and Termination:

As provided in the Safe Drinking Water Act, "section 14(a) of the Federal Advisory Committee Act (relating to termination) shall not apply to the Council." 42 U.S.C. § 300j-5(d). However, the Charter is subject to the renewal process upon the expiration of each successive two-year period following the date of enactment of the Act establishing this Council.

11. Member Composition:

NDWAC will be composed of fifteen (15) members who will serve as Special Government Employees (SGE). Members will be appointed by EPA's Administrator after consultation with the Secretary of the Department of Health and Human Services. As required by the Safe Drinking Water Act, five (5) members will be appointed from appropriate State and local agencies concerned with public water supply and public health protection; five (5) members will be appointed from private organizations or groups demonstrating an active interest in the field of water hygiene and public water supply, of which two (2) members will represent small, rural public water systems; and five (5) members will be appointed from the general public. 42 U.S.C. § 300j-5(a). .

In addition, up to five (5) Federal employees will be appointed as technical advisors to the Council. The technical advisors may include individuals representing the EPA's Science Advisory Board (SAB), the Centers for Disease Control and Prevention's (CDC) National Center for Environmental Health and National Center for Infectious Diseases, and such additional Federal officials as the EPA deems necessary for the NDWAC to carry out its function. Technical advisors may participate in Council discussions, but not Council deliberations.

12. Subgroups:

EPA, or NDWAC with EPA's approval, may form NDWAC subcommittees or working groups for any purpose consistent with this charter. Such subcommittees or working groups may not work independently of the chartered committee and must report their recommendations and advice to the entire Council for full deliberation and discussion. Subcommittees or working groups have no authority to make decisions on behalf of the chartered Council and they cannot report directly to the Agency.

13. **Recordkeeping:**

The records of the committee, formally and informally established subcommittees, or other subgroups of the committee, shall be handled in accordance with NARA General Records Schedule 26, Section 2 and EPA Records Schedule 181 or other approved agency records disposition schedule. Subject to the Freedom of Information Act, 5 U.S.C. § 552, these records shall be available for public inspection and copying, in accordance with the Federal Advisory Committee Act.

DEC 11 2012

Agency Approval Date

DEC 14 2012

Date Filed with Congress

AL 13-000-0270

UNITED STATES ENVIRONMENTAL PROTECTION AGENCY
WASHINGTON, D.C. 20460

MAR 13 2013

OFFICE OF THE
CHIEF FINANCIAL OFFICER

The Honorable Harold Rogers
Chairman
Committee on Appropriations
U.S. House of Representatives
Washington, D.C. 20515

Dear Mr. Chairman:

I am transmitting the U.S. Environmental Protection Agency's response to the June 2012 Government Accountability Office report entitled, *Anthrax – DHS Faces Challenges in Validating Methods for Sample Collection and Analysis* (GAO-12-488). The EPA prepared this response pursuant to 31 U.S.C. 720. The EPA appreciates the GAO's diligence and efforts in its review of this highly visible and important program.

The GAO conducted this review to identify the extent to which (1) the Department of Homeland Security's actions have addressed the GAO's recommendations in its earlier report regarding sampling, (2) the environmental sampling methods for *B. anthracis* spore detection in initial public health sampling and microbial forensic investigations have been validated, and (3) any challenges remain to completing validation.

The GAO has made three recommendations in this report, two addressed to the Secretary of the DHS and the third directed to the Administrator of the EPA and the Secretary of the Department of Health and Human Services. The GAO has made recommendations that DHS (1) update the strategic plans and roadmap's scope and timelines and (2) complete the validation project and (3) that the HHS and the EPA should support achieving the DHS's goal of validated sampling methods and the development of a mutually acceptable statistically-based sampling approach.

Below are the EPA's most significant comments on the report's recommendation for the development of a mutually acceptable statistically-based sampling approach.

GAO Recommendations

To ensure that federal agencies have validated sampling methods for detecting *B. anthracis* in indoor environments and—in the case of negative results—the option of using appropriate sampling approaches to make statistical confidence statements about the likelihood that a building is free of contamination when potentially there has been a low-level release, we

recommend that the Secretary of Homeland Security take steps to complete the validation project. Statistically-based sampling designs for such purposes would encompass any sampling with a statistical basis, including a probabilistic only approach as well as one that combines judgmental and probabilistic sampling. Achieving a sufficiently rigorous validation of the sampling methods and ensuring that statistically rigorous and mutually acceptable sampling approaches are available will provide options that will better prepare decision makers to respond to a future bioterrorism incident.

DHS should

- update the strategic plan and its roadmap with an agreed-on scope and revised timelines and
- complete the validation project, including validating the collection methods in a laboratory setting in a manner that determines the potential sources of variation in collection method performance, including variation that could be introduced by individual samplers, and related ongoing studies.

We also recommend that the Secretary of the Department of Health and Human Services and the Administrator of the Environmental Protection Agency support DHS in its goal of achieving (1) validated sampling methods to understand the limitations of the data that would be provided to decision makers, and (2) a mutually acceptable statistically-based sampling approach that can be employed when decision makers—such as Incident Commanders and others—conclude that statistical confidence statements need to be made about the level of contamination in a particular indoor environment.

EPA Response

The EPA does not agree with the GAO's recommendation. The EPA has significant concerns about the GAO's recommendation of a statistically-based approach for anthrax contamination, including its three recommendations that flow from that statistically-based approach. The EPA's concerns are based on (1) the successful real-world and multi-agency exercises that have used targeted sampling, (2) the difficulties both in achieving, and on-the-ground implementation of, the statistical-based approach, and (3) existing larger and more critical gaps needed to be filled in order to address *B. anthracis* decontamination.

Given today's realities, a statistically-based approach is not necessary from a scientific perspective, nor is it needed to make statistical confidence statements about the level of contamination in a particular indoor environment.

From a scientific perspective, studies such as those conducted at Idaho National Laboratories have continued to reinforce the effectiveness of targeted sampling that the EPA used in its 2001 Capitol Hill response. The GAO's report references the INL-1 and INL-2 experiments. These experiments validated that use of targeted sampling resulted in the identification of all contaminated locations but with a much smaller number of samples compared to statistical sampling.

In addition, the EPA is concerned that the GAO's recommendations do not consider that the real-world response on Capitol Hill in 2001 was successful due to the implementation of targeted sampling.[1,2] Although the GAO's final report references the anthrax response in 2001 which notably was the EPA's first time to respond to such an incident, it does not mention that the response was successful without any subsequent illnesses.

The GAO's recommendation is based on an assumption that there is a need for statistical sampling in order to enable decision makers to make determinations regarding decontamination. However, the GAO's recommendation does not take into account the time a building may be shut down while decision-makers wait on laboratory analysis and the costs that would be incurred. Currently, and for the foreseeable future, the environmental laboratory analytical capacity and the manpower or resources to conduct the sampling that is required for a timely response do not exist. On the other hand, the EPA typically collects targeted composite samples thus allowing us to collect from a similar number of locations as a statistical sampling but with less overall samples. For example, if an area requires 100 samples to make a statistical confidence statement, we can collect 25 4-point composite samples (equaling 100 locations). Therefore, we have reduced the number of individual samples by 75 percent and the time it takes to collect them as well. This further reduces the number of individual samples to be analyzed and reduces the chance that contamination will spread to uncontaminated sites. In other words, it is appropriate to designate that collection activities at composite sampling locations are conducted room by room so that if contamination is spread it is confined to that room.

To support its recommendations, the GAO's final report advises that rather than take a simplistic approach to sampling, we should be relying on professional samplers with substantive knowledge to devise sampling approaches. This is exactly what the EPA intended in its argument for targeted sampling. In statistical sampling, a software tool drives the number of samples based on a desired confidence level – not the judgment of a professional sampler.

With respect to development of the statistically-based approach, the GAO's recommendations are not clear in its expectations from the EPA. For example, the GAO explains that the Visual Sampling Plan software already includes a Pacific Northwest National Laboratory validated sampling approach for a random and a combined judgmental and random (CJR) sampling approach. Specifically, the report states, "the CJR algorithm can be used to determine the required number and location of probability based samples to provide a specified confidence that a specified level of contamination is not exceeded, including very low levels." It is not clear what

[1] Although there were two instances when samples were collected that yielded negative results; it was the result of not following appropriate sampling protocols. When the sample collection was repeated, contamination was in fact found, the discrepancy was immediately resolved. The initial failure to capture contamination in the samples could occur in either statistically-based or targeted sampling, and therefore, does not support the use of a statistically-based approach over a targeted approach.

[2] There are a couple of typos in the final report's discussion of the rapid-viability PCR method for detection of live, virulent *B. anthracis* spores in wipe, air, and water samples, page 89. The spore background levels are off by significant factors due to dropped superscripts. Live *B. anthracis* Ames spores detected in heat-killed *B. anthracis* spore backgrounds of "106 colony-forming units per sample" should be "10^6 colony-forming units per sample" and in the combined non-target backgrounds of "103 live *B. atrophaeus* subspecies *globigii* and 106 live *Pseudomonas aeruginosa*" should be "10^3 live *B. atrophaeus* subspecies *globigii* and 10^6 live *Pseudomonas aeruginosa*".

AL 13-000-0650

UNITED STATES ENVIRONMENTAL PROTECTION AGENCY
WASHINGTON, D.C. 20460

JAN 29 2013

OFFICE OF THE
CHIEF FINANCIAL OFFICER

The Honorable Harold Rogers
Chairman
Committee on Appropriations
U.S. House of Representatives
Washington, D.C. 20515

Dear Mr. Chairman:

I am transmitting the U.S. Environmental Protection Agency's response to the October 2012 Government Accountability Office report entitled, *Rural Water Infrastructure, Additional Coordination Can Help Avoid Potentially Duplicative Application Requirements* (GAO-13-111). The EPA prepared these responses pursuant to 31 U.S.C. 720.

The EPA is fully committed to working with its federal and state partners to ensure that federal funding supports the missions of our respective agencies and is accessible to communities in need. The agency supports the GAO recommendations with the caveat that there are limitations to the EPA's authority and what we can require of our state partners within the Clean Water State Revolving Fund and Drinking Water State Revolving Fund programs. The GAO recommendations are summarized below, followed by the EPA's response and a statement of action reflecting current interagency collaboration efforts.

GAO Recommendation:

To improve coordination and to reduce the potential for inefficiencies and duplication of effort, we recommend that the Secretary of Agriculture and the Administrator of the EPA take the following three actions:

- ensure the timely completion of the interagency effort to develop guidelines to assist states in developing their own uniform preliminary engineering reports to meet federal and state requirements;

- work together and with state and community officials to develop guidelines to assist states in developing uniform environmental analyses that could be used, to the extent appropriate, to meet state and federal requirements for water and wastewater infrastructure projects; and

- work together and with state and community officials through conferences and workshops, Webinars, and sponsored training to reemphasize the importance of coordinating in all four key areas in the 1997 memorandum.

EPA Response

The EPA concurs with the recommendation and is taking the following actions:

In February of 2012, the EPA began participation in an interagency workgroup of federal and state partners, including representatives from United States Department of Agriculture, the United States Department of Housing and Urban Development, the Bureau of Indian Health Service in the United States Department of Health and Human Services, and 13 states. The purpose of this workgroup is to establish uniform best practices for preliminary engineering reports across funding agencies. The workgroup has produced a draft interagency memorandum that explains the purpose of the workgroup, a general outline of a preliminary engineering report, and a detailed template of each desired component. This is an ongoing project and federal partners will continue to cooperate as the draft documents undergo review and are finalized. The EPA anticipates that these materials will be ready to share with state partners in early 2013.

The EPA and its federal and state partners are committed to conducting the necessary outreach to ensure that these best practices are fully understood and can be utilized by state partners. A first step in this process was undertaken at the fall Council of Infrastructure Financing Authorities conference on November 11-13, 2012. The EPA and the USDA took part in a panel that discussed current collaboration efforts, including the forthcoming preliminary engineering report template and the 2011 memorandum of agreement focusing on the sustainability of rural water and wastewater systems.

The EPA believes that the publication of the template will be a significant step forward in attempting to establish greater consistency among the preliminary engineering reports submitted by applicants. Although the EPA fully endorses this collaborative effort, adopting the template for the SRF purposes will be left to the states' discretion because preliminary engineering reports are not a federal requirement for the SRF programs. If the template is adopted, states may not require it for every SRF project or may waive portions of the template that are not applicable.

Environmental review requirements for the CWSRF program are detailed in 40 CFR 35.3140. Requirements for the DWSRF are detailed in 40 CFR 35.3580. In practice, states adhere to a "NEPA-like" state environmental review process. A state may elect to apply the procedures at 40 CRF Part 6, Subpart E and related subparts, or apply its own "NEPA-like" SERP for conducting environmental reviews. Before a state may utilize a "NEPA-like" process it must first receive approval from the appropriate EPA region. The purpose of allowing states to adopt their own "NEPA-like" SERP was not to deviate from NEPA, but rather, to delegate environmental review responsibility to the states while still conforming to NEPA.

While we cannot require states to use a more uniform environmental review process, the EPA will work with the USDA to determine what specific issues they have with the SRF environmental analyses. The agency's tentative goal is to schedule an interagency staff level meeting in early 2013. After this information has been obtained, we can work with state partners to examine the possibility of whether their SERP can be modified or whether some other option can be pursued.

The agency looks forward to continued dialogue with the USDA to explore how we can encourage states to continue the development of policies and processes that align with the key areas of the 1997